ALTIGEN®
COMMUNICATIONS

MaxACD Administrator™ Manual

July, 2011

WARNING! Toll fraud is committed when individuals unlawfully gain access to customer telecommunication systems. This is a criminal offense. Currently, we do not know of any telecommunications system that is immune to this type of criminal activity. AltiGen Communications, Inc. will not accept liability for any damages, including long distance charges, which result from unauthorized and/or unlawful use. Although AltiGen Communications, Inc. has designed security features into its products, it is your sole responsibility to use the security features and to establish security practices within your company, including training, security awareness, and call auditing.

NOTICE: While every effort has been made to ensure accuracy, AltiGen Communications, Inc., will not be liable for technical or editorial errors or omissions contained within the documentation. The information contained in this documentation is subject to change without notice.

This documentation may be used only in accordance with the terms of the AltiGen Communications, Inc., License Agreement.

MaxACD for Lync, MaxACD Administrator, MaxAgent, MaxAgent for Lync, MaxSupervisor, MaxReports, VRManager, and Enterprise Manager are trademarks or registered trademarks of AltiGen Communications, Inc. All other brand names mentioned are trademarks or registered trademarks of their respective manufacturers.

AltiGen's products are protected under one or more of the following U.S. patents, with other U.S. patents pending: 6532230; 6192344; 6292549; 6493439; 6909780; 6738465; 6754202; 6766006; 6928078; 6909709; 6956848; 7058047; 7013007; 7027578; 7280649; 7308092.

AltiGen Communications, Inc.
410 East Plumeria Dr.
San Jose, CA 95134
Telephone: 888-AltiGen (258-4436)
Fax: 408-597-9020
E-mail: info@altigen.com
Web site: www.altigen.com

Contents

About This Manual

This manual shows administrators how to configure AltiGen's MaxACD for Lync using the **MaxACD Administrator** application.

Related MaxACD publications include:

- MaxAgent for Lync Manual
- MaxSupervisor Manual
- Advanced Call Router Manual
- MaxInsight Manual
- MaxReports Manual

CHAPTER

1

Overview

MaxACD for Lync is AltiGen’s system software that supports AltiGen’s MaxAgent for Lync.

MaxAgent for Lync is a robust workgroup call handling application that works in tandem with Microsoft Lync Client. The product is designed to provide contact centers with the essentials to service, respond and track performance of contact professionals. MaxAgent features are described below.

MaxACD for Lync is designed with an intuitive easy-to-use graphical user interface, **MaxACD Administrator**, so IT staff can easily manage the system and reduce administrative costs. Since MaxACD is IP-enabled and modular, call-centric businesses are protected against growing out of their investment.

Key features of the MaxACD for Lync system are listed below in the following categories:

- System features
- Automatic call distribution features
- Auto-attendant features
- Voice mail features
- Administrative features
- Voice over IP features
- AltiGen’s additional ACD-related applications
- Capacities

Features are listed in alphabetic order in each category.

MaxACD Features

Account Codes - allows the user to input an account code on each call to track telephone usage in order to bill back to clients or create a record of calls specific to a project and to budget and forecast expenses. **Forced Account Codes** force the user to input an account code on each call to track telephone usage. The administrator can configure which extensions are required to enter an account code, and also configure the option to require an account code for long distance calls and international calls, but not local calls. An administrator also can block the display of the account code table in client applications. Users can be prevented from seeing account codes they don’t need to see.

Automatic Dialing Plan Rules- Administrators can configure a call return rule based on the country in which they reside. Applies to call return from Caller ID, Zoomerang, and making a call from Microsoft Outlook.

Business Hours Profile - allows for setting morning and afternoon business hours for each day of the week. Multiple business hours can be configured in a system. Also, multiple Business Hours profiles can be assigned to DNIS Routing and Trunk In Call Routing entries.

Busy or Ring No Answer Call Handling - sends calls to voice mail, another extension, or **AA** if the called extension or group is busy or does not answer.

Caller ID Routing - the system administrator can define Caller IDs in a routing table and set different routing options.

Dial Last Caller - allows user to dial the last caller using #69.

Directory Name Announcement - the extension user's directory name will be announced to the caller before the call rings to a phone.

Extension Availability Display - allows users of MaxAgent for Lync to select from Lync Client's set of pre-defined availability statuses. These statuses are synchronized with Lync Client.

Holiday Routing - routes inbound DNIS and trunk calls on designated holidays to specified destinations. You can create separate routes for business and non-business hours on half-day holidays. Multiple Holiday Profiles can be configured in a system. Also, multiple Holiday Profiles can be assigned to DNIS Routing, Caller ID and Trunk In Call Routing entries.

Line Park—allows for a set of 99 lines to be used as a park pool, where trunk incoming calls can be parked automatically, (by routing/call handling treatment in MaxAdministrator). Park Lines are organized into groups, with up to 99 groups supported. Parked Lines can be assigned to an IP phone programmable key for call pickup. Line Park group has busy queuing and time out transfer options.

Multi-lingual support - supports multiple sets of system and custom language phrases. Up to 9 different sets of language phrase can be configured. A language preference tag can be assigned to the extension user or selected by the incoming caller. The system plays the specified language when the extension user accesses system features.

Music on Hold—allows callers to hear music or pre-recorded messages while waiting on hold.

Out Call Routing Configuration—allows outgoing calls to be directed to particular trunk routes, based on a configured dialing pattern.

Outside Call Blocking—when this feature is enabled, access to outside lines is temporarily disallowed.

Transfer Caller to AA - allows a user to transfer a call to an AA by pressing **FLASH #15** and then the 2- or 3-digit AA number.

Workgroup Call Pickup - allows agent or supervisor to pick up a specific call in queue.

Automatic Call Distribution Features

Automatic call distribution (ACD) features include:

Advanced Queue Management Application - enables advanced queuing options:

- One-level AA menu selection from queue
- Advanced queue overflow for configuration of overflow conditions and actions

After Hours Handling for Workgroups - a workgroup can be assigned a Business Hours Profile through MaxAdministrator. Also, after hours routing decisions can be configured for each day of the week. When a call is forwarded to this workgroup after hours, the call is routed automatically, based on the routing decision for that day of the week.

Agent Login/Logout - allows workgroup members to log in and out of a group so that incoming calls bypass the workgroup member (agent) who has logged out and the call is automatically routed to other agents who are logged in.

Agent Logout Reason Codes - allows a workgroup member to enter a reason code when signing off. Up to 20 reason codes may be defined.

Agent Set to Not Ready When RNA - when a workgroup call rings an agent and is not answered, this feature automatically sets the agent state to Not Ready.

Agent Auto Logout When RNA - when a workgroup call rings an agent and is not answered, this feature automatically sets the agent state to Logout for that particular workgroup.

Call Queuing - places caller in a queue to wait until an ACD group member becomes available.

Call Queue Announcement - before a call enters a workgroup queue, the system announces the expected wait time or call queue length to the caller.

Call to Queue Alert - agents can be alerted via a beep and a screenpop when a call enters the workgroup queue.

Inter Call Delays - can be used to set delays before the system sends the next call to an extension after the agent finishes an outbound call or other non-workgroup call activity.

Login/Logout/Keep Login Status on system startup or reboot - all group members can be set to the "Login" or "Logout" state at system startup or reboot. By default, group members are set to "Keep Login Status."

Multiple Queue Announcements - allows each group to have its own set of unique audio announcements. Up to five announcements can be configured for each group. The intervals between announcements can also be configured.

Multiple Workgroup Membership - allows each extension to belong to multiple groups. The system can be configured with a maximum of 64 groups (workgroups).

Multiple Workgroup Log In and Log Out - lets group members quickly log in and out of multiple groups. (#54 and #56)

Picking/Transferring Calls from Group Queue - enables an extension to pick any call in queue using MaxAgent. MaxSupervisor is also able to transfer a workgroup queued call to any extension, workgroup, AA, voicemail or outside number.

Priority Queuing - allows for calls in queue to be associated with a priority. The call priority can be assigned though Caller ID routing, DNIS routing, AA, or other add-on applications. Call distribution is based on the call priority and queue time. Call priority can be escalated if queue time exceeds a certain limit.

Queue Announcement - before a call is sent to a group queue, expected wait time and call position are announced.

Quit Queue Option - a caller can press "#" or "0" to leave a workgroup queue to transfer to group voice mail, AA, extension, another group, or an operator.

Ready/Not Ready - agent can set state to "ready" (#90) or "not ready" (#91) to inform the system whether the agent is able to receive the next call while logged in to a workgroup.

Real Time Monitoring -

- Workgroup’s calls in queue, longest queue time, # of calls exceed service level threshold, and service level
- Number of agents in Login, Logout, Idle, Busy, Not Ready, Wrap-up, DND/FWD, or ERROR state.
- Workgroup and Agent’s performance summary data output to client applications.

Service Level Threshold - a time value for callers waiting in queues. The performance statistics show when workgroup calls are queued for longer than a prescribed value.

Skill-Based Routing - this feature includes the following capabilities:

- Assigning skill level requirement (SKLR) to caller
- Assigning skill level (SKL) to agent
- Matching caller’s SKLR to agent’s SKL
- Setting skill coverage and escalation rules

Supervisor Silent Listen - allows a workgroup supervisor to silently listen to a call between workgroup agent and caller. Personal calls can also be silently listened to by a workgroup supervisor.

Supervisor Barge In - allows a workgroup supervisor to barge into a call between workgroup agent and caller. Personal calls can also be barged in to by a workgroup supervisor.

Supervisor Coach (Whisper) - allows a workgroup supervisor talk to a workgroup agent without the other party hearing.

Queue Overflow Handling - routes incoming calls to an alternate destination when the queue reaches one of the following conditions:

- Calls in queue exceed defined limit
- Longest queue time exceeds defined limit
- Specified percentage of calls in queue with queue time longer than defined service level threshold

Workgroup activity data logging - in addition to CDR data, the following data are logged to a database during workgroup operation:

- Agent activity - Login, Logout, Not-Ready, Wrapup, DND/FWD, Error
- Agent’s call summary per workgroup
- Agent’s call statistics for all workgroups
- Workgroup operation summary

Workgroup Activity Monitoring - allows real-time monitoring of workgroup information—group status, call queue status, details of group queue entries, and agent status. Activity summary is available through a group view window in MaxACD Administrator, MaxAgent, and MaxSupervisor.

Workgroup Call Distribution - calls can be distributed to the first available group member, or among group members according to the following options:

- Ring First Available Member
- Ring Next Available Member
- Ring All Available Members
- Ring Longest Idle Member
- Ring Average Longest Idle Member
- Ring Fewest Answered Calls

- Ring Shortest Average Talk Time
- Skill-Based Routing

Wrapup Time - allows a group member some time in between calls to wrap up on notes, prepare for the next call, or log out of the group. This wrapup time is configurable on a per-agent basis.

Auto Attendant (AA) Features

The AA features provide quick and courteous processing of all incoming calls. An AA can be configured to serve as a primary attendant or as a backup to a receptionist.

AA features include:

Dial By Name - allows a caller who does not know your extension number to spell your name using the telephone key pad. The system will search the Directory and make a match on the name to connect the caller to the intended party’s extension. The caller can match first OR last name when dialing by name.

Data-Directed Routing - allows the routing of calls directed by the caller’s input (digit or text). Third-party applications can be used to route incoming calls based on caller information.

Digit Collection - caller can be prompted to enter numbers, which are then collected and used for routing the call.

Multiple AA Support - allows up to **255** auto attendants.

Programmable Time-Out Handling - allows the administrator to select the action the system should take if there is no digit dialed by the caller within a specified number of seconds.

Set Call Priority - allows the administrator to assign a priority level to an AA menu.

Set Skill Level Requirement - allows the administrator to assign a skill level requirement to an AA menu.

Voice Mail Features

The Voice Mail System is a message management system that provides the calling and the called parties with enhanced communication features. It allows greater accessibility, faster reply time between parties, and reduces the frustration of telephone tag.

The voice mail system includes the following features:

Configurable voice mail playing order - Administrators can configure users’ voice mailboxes to play the oldest or the newest message first.

Disable a Mailbox - voice mailboxes can be disabled so that callers cannot leave messages.

Future Delivery - allows users to record a message to be delivered at a specific time and date in the future, up to one year in advance.

Information Only Mailbox - a mailbox can be configured to announce customized pre-recorded information when accessed. This mailbox does not allow callers to leave a message, but only to listen to the message announcement (personal greeting) from the mailbox. To repeat the message, callers are instructed to press the **#** key.

Making a Call from the Voice Mail System - allows users to make a call from within the Voice Mail System by pressing **#** at the Main Menu and entering the internal extension or external phone number. This is especially useful while traveling where users can respond to all messages and make *other* calls not associated with a message, all with *one* call into the Voice Mail System. This can result in significant savings. The use of this privilege is configurable on a per-user basis.

Message Management - receives, sends, forwards, deletes, and replies to messages.

Message Notification - designed to alert you of new voice messages in your mail box by calling an extension, phone or pager number. A notification schedule can be set for business hours, after business hours, at any time or at a specified time. You have an option of being notified of all messages or only urgent messages.

New and Heard Voicemails Announced - Heard voicemails are announced, as well as new and saved voicemails, when users access voicemail.

Personal Greeting - allows users to record a personal greeting in their own voice to be played when callers reach their voice mail.

Press "0" Option for Extension in Voice Mail - allows a caller to press "0" while listening to an extension's greeting. The "0" can be configured by the administrator to forward the user to operator or other destinations.

Priority Delivery - allows caller to set the priority of message delivery such as normal or urgent.

Private Messaging - allows users to leave a private message in their voice mail for the expected caller.

Reminder Calls - are used to remind you of important meetings, things to do or people to call.

Remote Access - allows users to access the Voice Mail System from outside by dialing into the AA and pressing **#** to log in.

Return to AA - after leaving a voicemail message and pressing **#** to send it, incoming trunk callers are prompted with the option to return to AA to try another path or person.

Set Call Forwarding from Voice Mail - users can set up Call Forwarding from within the Voice Mail System. This allows users to set up Call Forwarding while away from the office.

Voice Mail Distribution List - allows the user to use system distribution lists or personal distribution lists for forwarding voice mail. Up to 100 distribution lists can be created. Each distribution list can have up to 64 entries, and any entry can be another distribution list.

Zoomerang - allows users to listen to messages in the Voice Mail System, make a return call to a party who left a message, and then return to the Voice Mail System to continue checking the next messages, all in a single call into the Voice Mail System. If the caller ID information is not captured, the user may enter the "call back" number manually.

Exchange Integration Features

Integration features include:

Exchange Integration - provides message synchronization between MaxACD and a Microsoft Exchange server on the LAN. This feature allows for dynamic synchronization of mail between the two servers so that deleted messages from one server get automatically deleted in the other server. Similarly, a new message sent to one server is transmitted to the other server. This way, the message can be accessed or deleted from either server. For example, when a voicemail message is deleted from MaxACD, it is automatically deleted from the Exchange server too.

Administration Features

System and administration features include:

AA Configuration File Export- lets you export your complete AA configuration to an html file.

AA Copy - An AA configuration can be copied, forming the template for a new AA.

Alerting - An announcement can be sent to Voice Mail when the e-mail server disk is full.

"Apply To" Feature - applies changes (only the field that was changed) to multiple extensions, trunks or channels instead of having to change them one at a time.

Call Detail Reporting (CDR) - the system collects and records information on outgoing and incoming phone calls, such as length of call, time of call, number of calls. This data is written to an internal database.

Configurable Emergency Number - For international use, allows the system administrator to set up country-specific emergency numbers.

DNIS Routing Tables - incoming trunk calls can be routed to an AA, extensions, workgroups, hunt groups, and so on, based on DNIS numbers configured in the system administration routing tables.

E-911 Calling Support - allows an administrator to designate a number of trunks for dedicated E-911 use.

Voice Mail Storage - can be placed on drives other than the system drive.

Emergency (911) Call Notification to Extension/Outside Number - when any extension dials an emergency number that gets routed through MaxACD, the system can make calls to pre-configured extensions or outside numbers. A system can have more than one emergency notification number configured.

Extension Password Protection for Application Logins - the system maintains a counter for each extension to track CTI client application login failures. When eight successive failures are reached, the system disables login connection for 1 to 24 hours to prevent password intrusion. Applies to MaxAgent, MaxSupervisor, and other add-on applications.

License Assignment - A **License** menu allows administrators to easily verify and assign licenses.

Log In and Log Out - An administrator can log in and log out a workgroup member from the Workgroup Configuration window in MaxACD Administrator.

Monitor List - lets you configure an extension's privilege to see other extension's call activity through MaxAgent.

Out Call Routing Configuration - allows outgoing calls to be directed to particular trunk routes, based on parameters assigned in the Out Call Routing table.

Remote Administration - a version of the MaxACD Administrator application that can be installed on a Windows XP/2003/2008 client computer to remotely administer one or more systems.

Voice over IP Features

VoIP features include:

Codec Profile - Multiple codec profiles with different settings can be created and applied to different locations. Each profile can have a different codec, jitter buffer, and packet length to accommodate different IP connections.

Dynamic Jitter Buffer - due to various delays in the IP network, audio packet streams may be delivered late or out of order. The system is able to buffer incoming packets and re-sequence them by maintaining a queue. This queue is adjusted dynamically to accommodate different network environment characteristics.

Echo Cancellation - due to bandwidth limitations and device loading, long delays may occur during packet delivery process, which worsens the echo effect voice speech. Echo cancellation is provided to maintain reasonable voice quality.

G.711 Codec - toll quality (64K) digital voice encoding, which guarantees interoperability and better voice quality.

G.723.1 Codec - a dual rate audio encoding standard, which provides near toll quality performance under clean channel conditions.

G.729 A+B Codec - speech data encoding/decoding standard of 8 Kbps.

Silence Detection and **Suppression** - when silence suppression is enabled and silence is detected, the system stops sending packets to the other side. The other side does not receive any packets and plays silence.

SIP Trunk Support - MaxACD enables AltiGen’s system to connect to IP-based trunking service providers via SIP.

Support for RFC 2833 (DTMF payload embedded with RTP) - Supported in SIP trunks only. This feature helps to resolve DTMF tone detection and regeneration when using G.723.1 or G.729 codec. Low bit rate compression will distort DTMF tone during compression. The far end device may not be able to recognize the DTMF digits. RFC 2833 specifies a separate RTP payload format to carry DTMF information to ensure the other side can recognize the tone properly.

Additional Workgroup-Related Applications

In addition to **MaxAgent for Lync**, the following workgroup-related applications are available from AltiGen:

MaxSupervisor - allows a workgroup supervisor to view an agent’s real-time activity, log in/log out an agent, view workgroup and agent operation statistics, listen/barge-in/coach an agent’s conversation.

- All workgroups a supervisor is monitoring are displayed in a single view, making it easy to see what’s happening in all groups at once.
- A graphical view (trend lines) displays workgroup statistics to help make better staffing decisions.
- Supervisors can check workgroup voice mails without needing a separate license or needing to log in as an agent.
- Color coded priority in queue
- Change caller’s priority
- Record agent’s conversation with indicator

MaxReports - application that can report an agent’s and workgroup’s operation details, including summary, analysis, and charting.

Advanced Call Router - a call handling application that matches incoming call data or collected digits against a customer’s CRM record to determine how to route the call. It has the capability to set call priority and caller’s skill level requirement.

MaxInSight - a workgroup performance application that provides call center managers and agents with the ability to track workgroup status and performance data from a wall-mounted LCD panel or from their PCs. MaxInSight includes the ability to see the following for single or multiple workgroups:

- Real-time queue status
- Real-time workgroup resource status
- Daily operation results
- Trends of data over time

VRManager - allows administrators/supervisors to convert, schedule backup/delete, and query recorded files.

SDK Tool Kit - offers a complete set of tools including APIs, documentation and sample programs, to enable a developer to begin programming rapidly and efficiently. It includes a self-installing CD-ROM containing AltiGen SDK software. Session-based licensing is required for both Basic API and APC API interfaces.

MaxCall - lets you set up transmitted Workgroup CID numbers for use by agents in the MaxCall application. Agents can then choose the appropriate CID for each call.

Capacities

Capacities for an All-in-One Single System

General Capacity

- Maximum 400 extensions
- Maximum 200 MaxAgent sessions
- Maximum 20 MaxSupervisor sessions

Call Center Capacity

- Maximum configurable agents per workgroup - 512
- Maximum active login agents per workgroup - 256
- Total configured agents per system including all workgroups - 1280
- Total agents seats (License/Head) per system - 512

Capacities for a Multi-Server System

General Capacity

- Maximum 2,000 extensions
- Maximum 400 MaxAgent sessions
- Maximum 20 MaxSupervisor sessions

Call Center Capacity

- Maximum configurable agents per workgroup - 512

- Maximum active login agents per workgroup - 256
- Total configured agents per system including all workgroups - 1280
- Total agents seats (License/Head) per system - 512

CHAPTER

2

System Requirements and Installation

This section describes the following:

- Operating System requirements
- MaxACD licenses
- Preparation for installation
- Installing MaxACD
- Uninstalling MaxACD
- Troubleshooting

System Requirements

The following operating systems are supported in MaxACD:

MaxACD Server

- Windows Server 2008 with SP1, 32-bit and 64-bit
- Windows Server 2008 R2 with SP1

MaxACD Administrator

- Windows Server 2003 with SP2
- Windows 7 (32-bit or 64-bit)
- Windows Server 2008
- A monitor with at least 1024 x 768 resolution or better

MaxACD Client Applications - Operating Systems

- Windows XP Professional
- Windows Vista Business Edition (32-bit and 64-bit)
- Windows 2008 (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- The following third-party integration software is supported by the MaxAgent for Lync client application:
  - Outlook 2007 and 2010

MaxACD Client Applications - System Requirements

- IBM/PC AT compatible system
- Microsoft .NET 2.0 framework or higher
- 2 GHz CPU
- 1 GB available hard drive disk space
- 1 GB RAM
- SVGA monitor (1024 x 768) with 256-color display or better
- Keyboard and mouse

CDRs

The following external CDR databases are supported:

- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 express

Note: Running SQL Server in a MaxACD machine is not supported.

Online Help

- Internet Explorer 6.0 or higher browser

Email Server Integration

- Microsoft Exchange Server 2008

MaxACD Licenses

This section lists the licenses available for components of MaxACD.

MaxACD for Lync Server Licenses (Bundle license *9Lxxxx...*)

- MaxACD for Lync License
- HMCP Media Server License x 1 (supports up to 600 G.711 codecs)
- HMCP Agent Supervision Session License x 20
- AltiReport License
- VRManager License
- Multi-Lingual License
- Advanced Call Router License
- SIP Trunk License x 300
- 10 MaxAgent for Lync Licenses
- 1 MaxSupervisor for Lync License

MaxAgent for Lync Licenses (Bundle license *9Axxxx...*)

MaxACD supports up to 256 agents.

- Station License x 1
- ACM Agent Seat License x 1
- MaxAgent Seat x 1

- Exchange Integration Seat License x 1
- MaxCall Seat x 1

MaxSupervisor for Lync Licenses (Bundle license *9Bxxxx…*)

- MaxSupervisor Seat License x 1
- MaxInsight Session License x 1

Additional Licenses

- HMCP G.711/G.723/G.729 VPR License
- Recording Seat
- Client Applications SDK Session License
- Trunk Control APC License
- Redundancy license

Preparation for Installation

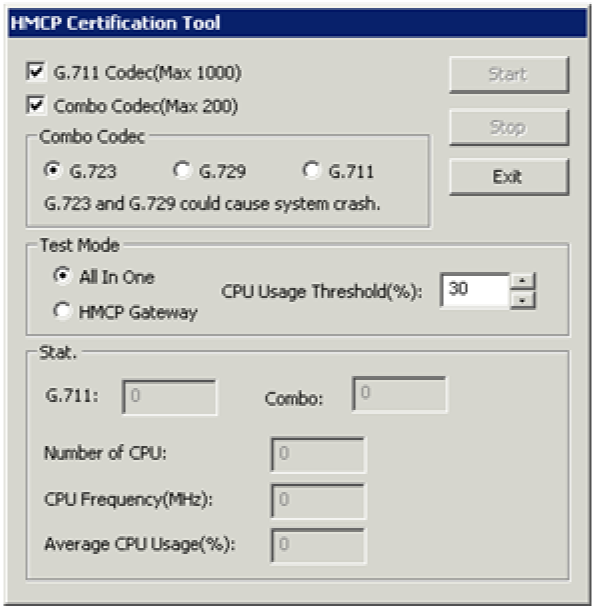
Before you start installing MaxACD, you need the following:

- **Windows Update:** Make sure your server has the recommended Windows Service Pack or Update.
- **MaxACD for Lync CD ROM:** The MaxACD CD ROM that contains the MaxACD for Lync program.
- **System Key:** The system key can be either a USB hardware security device that must be attached to the server MaxACD is running on, or it can be a soft system key.
    - You cannot use both a hardware device and the soft system key at the same time.
    - When using a soft system key, the MaxACD system will need to be a member of an Active Directory domain.
- **Software license key:** A 20-digit key located on the front of the End User License Agreement.

Run the HMCP Certification Tool

Before you begin the installation process, run the AltiGen HMCP Certification tool to make sure your system can run MaxACD.

1. In the installation CD, open the folder **HMCP Certification Tool**.
2. Double-click *setup.exe* in that folder to run the tool.



HMCP Certification Tool

☑ G.711 Codec(Max 1000)

☑ Combo Codec(Max 200)

Combo Codec

● G.723 ○ G.729 ○ G.711

G.723 and G.729 could cause system crash.

Test Mode

● All In One

○ HMCP Gateway

CPU Usage Threshold(%): 30

Stat.

G.711: 0

Combo: 0

Number of CPU: 0

CPU Frequency(MHz): 0

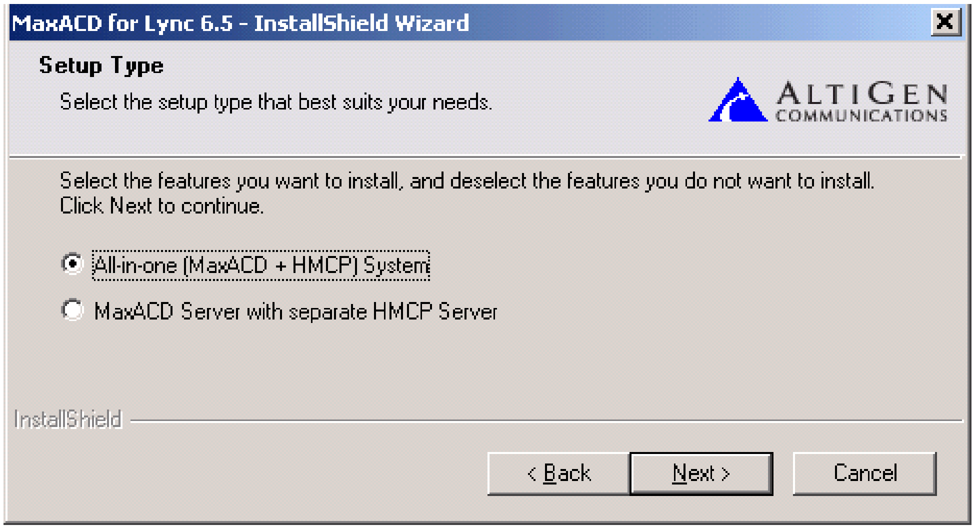
Average CPU Usage(%): 0

Figure 2-1. The HMCP Certification Tool

3. Choose the desired codec configuration. We recommend the following default settings for CPU Usage Threshold:
    - For an all-in-one system (all components on the same server): 30%
    - For systems with a dedicated HMCP: 70% (by default)
    - Do not set the value higher than 70%; if you do, unexpected results may occur.
4. Click **Start**. The tools begins to analyze your system; this process may take a few minutes.
5. When the analysis is complete, a window opens to show you the recommended number of G.711 codec resources and combo codec resources. Make a note of these results, as you will use them when configuring your system.

Installing MaxACD

To install MaxACD, insert the MaxACD for Lync CD ROM into the CD ROM drive of the server and follow the instructions on the screens. At the third screen, select a setup type:


MaxACD for Lync 6.5 - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Select the features you want to install, and deselect the features you do not want to install. Click Next to continue.

● All-in-one (MaxACD + HMCP) System

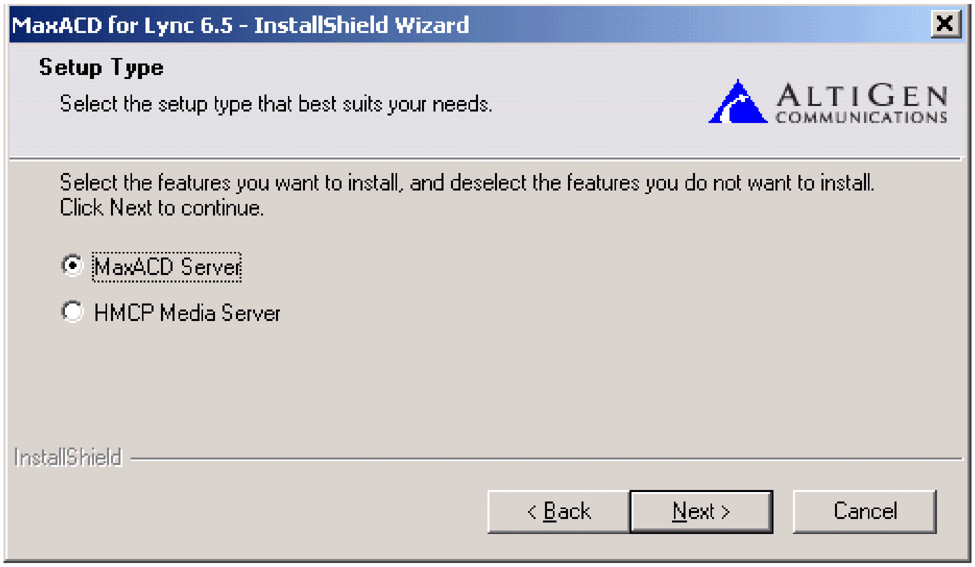
○ MaxACD Server with separate HMCP Server

Figure 2-2. MaxACD Installation dialog box

- **All-in-one (MaxACD + HMCP) System Installation:** Select this option if MaxACD will be operating on a single server. (This is a common configuration.)
- **MaxACD Server with Separate HMCP Server:** Select this option if the MaxACD Server and HMCP servers will be running in different chassis in an enterprise deployment. On the next screen you can select which components to install.

Installing MaxACD and HMCP Separately

You will choose which components to install.


MaxACD for Lync 6.5 - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Select the features you want to install, and deselect the features you do not want to install. Click Next to continue.

● MaxACD Server

○ HMCP Media Server

Figure 2-3. Setup Type Installation dialog box

- **MaxACD Server:** Select this option to install MaxACD to the server. You will need a dongle for the MaxACD server. MaxACD provides the following functions:
  - ACD Call Control
    - Call Distribution, Queueing, Routing, Call Handling, etc.
  - System Management
    - Configuration and Directory
    - Phrases and Prompts (System, Custom, Personal)
  - Feature Server
    - Voice Mail Server
    - Call Center Feature Server
    - CTI Server
    - Exchange Integration Server
    - CDR Server
- **HMCP Media Server:** If you have a small- to medium-size call center (no more than about 200 agents), you can install MaxACD and HMCP Media Server in the same machine. You can also install them in different machines, especially if you plan to grow your call centers.

  If you have more than 200 agents, install HMCP Media Server and MaxACD on different servers.

Installing Administrator on a Network Client

MaxACD Administrator can be installed on a client workstation, providing the ability to manage the MaxACD server remotely. The system running MaxACD Administrator and the MaxACD server must be on the same Windows domain.

When you install MaxACD Administrator on a machine that is not a MaxACD server, it does not contain the switching, SMTP/POP3 server, messaging agent, AltiBackup, and Exchange integration services that are included in the full MaxACD installation. Remote MaxACD Administrator does *not* utilize the System Data Management or Shutdown Switching Service functions on the MaxACD system.

To install MaxACD Administrator on a client workstation:

1. Insert the MaxACD CD-ROM into the appropriate drive.
2. Run **SETUP.EXE** from the MaxACD Administrator folder.
3. Follow the instructions on the screen.

Uninstalling MaxACD

To uninstall MaxACD, be sure to stop all MaxACD-related services before uninstallation. To do this, run MaxACD Administrator, log in, and select **Services > Shutdown Switching** from the menu.

In the event that the auxiliary services were not stopped, stop them one at a time in Windows, using the **Start > Programs > Administrative Tools > Services** applet.

Then go to **Start > Programs > Control Panel > Add/Remove Programs**, and select **MaxACD for Lync** and click **Remove**.

Lync Front-end Server Adjustments

During installation, you specified the Lync server proxy IP addresses. If you need to change either of those addresses in the future, follow these steps:

1. In Windows, choose **Start** > **All programs** > **AltiGen Lync Server Proxy** > **AltiGen Lync Server Proxy Configuration**.
2. In this tool you can add a new IP address, edit an existing address, or remove an address as needed. You can also change the registration information. After you make your changes, click **Apply**.

Troubleshooting (Error Messages)

Use this table for troubleshooting error messages encountered during software installation.

Error Message	Solution
Copy activation file failed.	Activation file (exctl) is not in the specified folder, is missing, or is corrupted. Make sure you select the correct file folder where the activation file is located and try again. If problem persists, you can manually copy the activation file to c:\AltiServ\db directory (if MaxACD is installed on the c: drive) and run the installation program again.
An error occurred during the move data process.	Make sure all MaxACD applications and services are stopped/closed before installing MaxACD.
Setup cannot append the AltiServ path because your existing system environment is too long. You must manually append the AltiServ path to your system environment path after finishing the MaxACD installation but before restarting your system.	Manually append c:\AltiServ\exe (if MaxACD is installed on c: drive) to your system environment path (through **Control Panel** > **System** > **Advanced** tab > **Environment Variables** > **System Variables**) after finishing the MaxACD installation but before restarting your system.
Unable to add AltiServ path to the system.	Manually append c:\AltiServ\exe (if MaxACD is installed on c: drive) to your system environment path (through **Control Panel** > **System** > **Advanced** tab > **Environment Variables** > **System Variables**) after finishing the MaxACD installation but before restarting your system

CHAPTER

3

Getting Around MaxACD Administrator

This chapter gives a brief overview of MaxACD Administrator, the application used to configure and administer the MaxACD for Lync software.

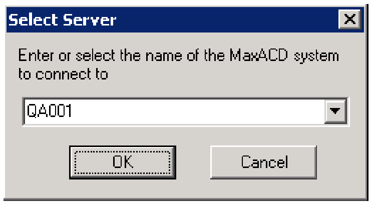
MaxACD Administrator has a graphical user interface with tabbed windows that makes it easy to use. Use it at the MaxACD for Lync system, or use it remotely on any other PC on the LAN.

Note: The commands **Services > Utilities > System Data Management**, and **Services > Shut Down All Services** cannot be performed remotely.

Logging In and Out

To configure and administer a MaxACD for Lync system, log in to MaxACD Administrator.

1. From the Windows **Start** menu, select **All Programs > MaxACD for Lync > MaxACD Administrator**. The Select Server dialog box opens:



Select Server

Enter or select the name of the MaxACD system to connect to

QA001

Figure 3-1. Select Server dialog box

2. Enter the name or IP address of the MaxACD system, and click **OK**. MaxACD Administrator opens.
3. To log in to MaxACD Administrator, click the **Login** button (the left-most button on the toolbar) or select **Services** > **Login**. You'll be prompted to enter the password and click **OK**.

The first time you log in, use the system default password, 22222.

Important: **To ensure system security, change the system password as soon as possible.**

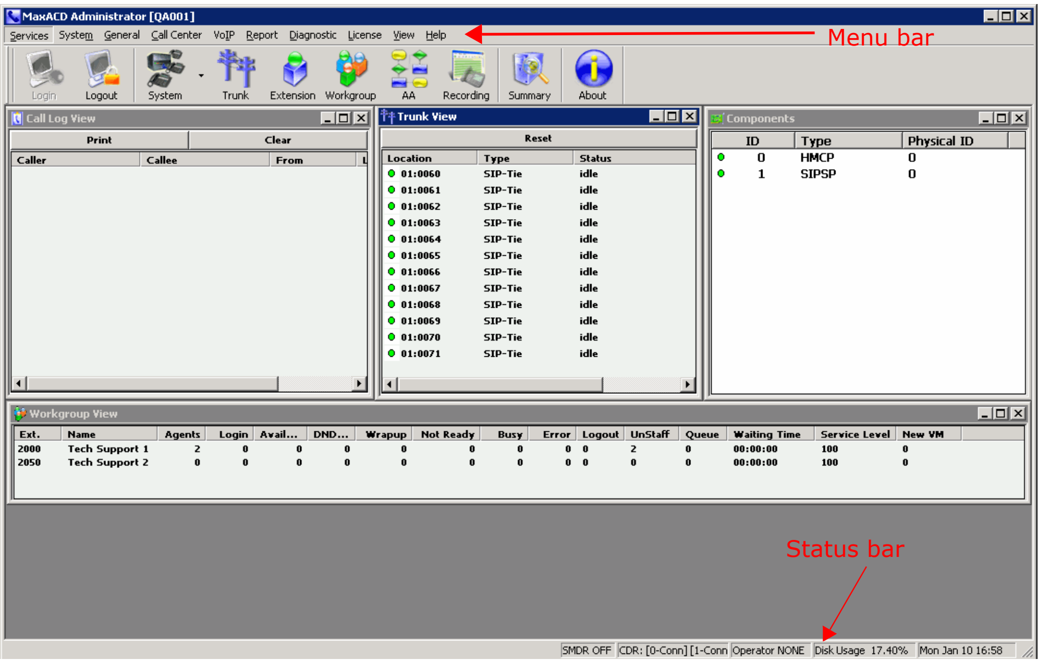
To log out, click the **Logout** button, or select **Services > Logout**.

Changing the Password

Select **Services** > **Change Password** to open a **Change Password** dialog box. You'll be prompted to type in and verify a new password, then click **OK**.

The MaxACD Administrator Main Window

When you run MaxACD Administrator, you'll see something like the following figure. You can resize, rearrange, or dismiss the individual windows within the main window.



Caller	Callee	From

Location	Type	Status
01:0060	SIP-Tie	idle
01:0061	SIP-Tie	idle
01:0062	SIP-Tie	idle
01:0063	SIP-Tie	idle
01:0064	SIP-Tie	idle
01:0065	SIP-Tie	idle
01:0066	SIP-Tie	idle
01:0067	SIP-Tie	idle
01:0068	SIP-Tie	idle
01:0069	SIP-Tie	idle
01:0070	SIP-Tie	idle
01:0071	SIP-Tie	idle

ID	Type	Physical ID
0	HMCP	0
1	SIPSP	0

Ext.	Name	Agents	Login	Avail...	DND...	Wrapup	Not Ready	Busy	Error	Logout	UnStaff	Queue	Waiting Time	Service Level	New VM
2000	Tech Support 1	2	0	0	0	0	0	0	0	0	2	0	00:00:00	100	0
2050	Tech Support 2	0	0	0	0	0	0	0	0	0	0	0	00:00:00	100	0

Figure 3-2.   MaxACD Administrator main window

The main menu bar is at the top. Below that are buttons for quick access to more commonly used configuration screens. A status bar at the bottom contains information on the current runtime status.

Note: If you are using Windows XP for MaxACD Administrator, the font that appears in the title of the view windows (Extension, Trunk, and so on) is in the Windows 2000 style font and will appear small. To adjust, change the Active Title font in Windows XP to Tahoma (or other font), or change the Window theme to Windows Classic.

The Main Menu

These are the menus and the functions found under each menu:

- **Services**
  Log in and log out, change password, access utilities (system data management, import and export an extension list from a .csv file, import extensions from Active Directory), shut down all services, and exit the application.

- **System**
  Opens windows where you can configure system settings, softswitch components, voice mail, auto attendants, multilingual support, call recording, and application extensions.
- **General**
  Opens windows where you can configure trunks, in call routing, out call routing, extensions, unassigned extensions, SIP devices, and line park.
- **Call Center**
  Opens windows where you can configure workgroups and agent logout reasons.
- **VoIP**
  Opens windows where you can configure the enterprise network and refresh the enterprise settings.
- **Report**
  Opens windows where you can view the system summary and IP traffic statistics and configure SNMP (simple network management protocol).
- **Diagnostic**
  Opens windows where you can view the trace, open the Trace Collector, and view the system log. For use by authorized technical personnel.
- **License**
  Opens windows from which you can manage licenses: a License Information window, where you can view installed licenses and your license key list, and from which you can add and register additional licenses; and a Client SEAT License Management window, where you can add and remove members from a license type.
- **View**
  Lets you show, hide, and set default alignment of the view windows, the toolbar, and the status bar. Opens the CT Proxy Monitor.
- **Help**
  Opens the Help window and shows the MaxACD for Lync and the MaxACD Administrator versions. Also gives you a link to the AltiGen Technical Support web site.

Quick Access Toolbar

Toolbar buttons give you quick access to frequently used functions.

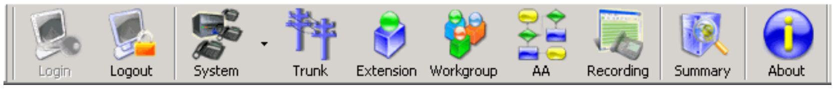


Figure 3-3. MaxACD Administrator quick access toolbar

From left to right, the toolbar buttons serve the following purposes:

Login. Opens the Password dialog box to log in to the system.

Logout. Logs out of the system.

System. Opens the System Configuration window, or the System menu.
Shortcut for **System > System Configuration**.

Trunk. Opens the Trunk Configuration window.
Shortcut for **General > Trunk Configuration**.

Extension. Opens the Extension Configuration window.
Shortcut for **General > Extension Configuration**.

Workgroup. Opens the Workgroup Configuration window.
Shortcut for **CallCenter > Workgroup Configuration**.

AA. Opens the AA Configuration window.
Shortcut for **System > AA Configuration**.

Recording. Opens the Recording Configuration window.
Shortcut for **System > Recording Configuration**.

Summary. Opens the System Summary window.
Shortcut for **Report > System Summary**.

About. Opens a window that displays version and file information. Gives information about the AltiGen Technical Support Web Site.
Shortcut for **Help > About MaxACD Administrator**.

Status Bar

The **Status Bar** at the bottom of the main window displays disk usage, the status of SMDR, the status of the call detail reporting log, the status of the operator, and current date and time.

The View Windows

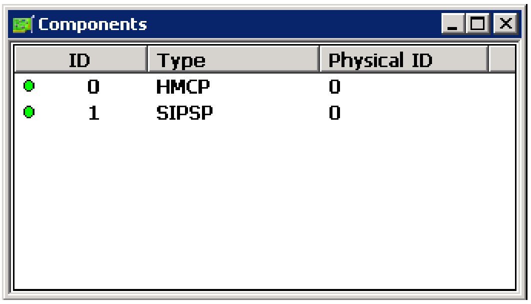
The MaxACD Administrator main window hosts a number of child windows that provide various views into the internal system real-time status.

Components View Window

The **Components** window displays the component types and their logical and physical IDs. For each installed component, it displays:

- The component’s logical ID (the sequential ID of the component assigned by the system).
- Component type

- The physical ID (including the ID of the component and the gateway ID).



	ID	Type	Physical ID
🟢	0	HMCP	0
🟢	1	SIPSP	0

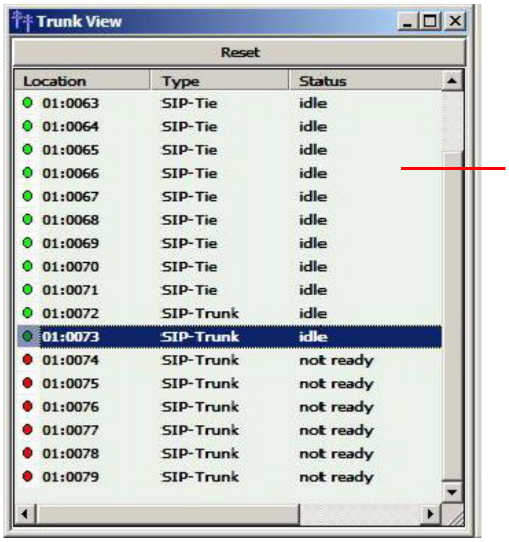
Double-click a component to open a configuration window for that component.

Figure 3-4. Components window

Click on any column heading to sort by that column. Click again to reverse the sort order.

Trunk View Window

The **Trunk View** window displays the status of all assigned trunks.



	Location	Type	Status
🟢	01:0063	SIP-Tie	idle
🟢	01:0064	SIP-Tie	idle
🟢	01:0065	SIP-Tie	idle
🟢	01:0066	SIP-Tie	idle
🟢	01:0067	SIP-Tie	idle
🟢	01:0068	SIP-Tie	idle
🟢	01:0069	SIP-Tie	idle
🟢	01:0070	SIP-Tie	idle
🟢	01:0071	SIP-Tie	idle
🟢	01:0072	SIP-Trunk	idle
🟢	01:0073	SIP-Trunk	idle
🔴	01:0074	SIP-Trunk	not ready
🔴	01:0075	SIP-Trunk	not ready
🔴	01:0076	SIP-Trunk	not ready
🔴	01:0077	SIP-Trunk	not ready
🔴	01:0078	SIP-Trunk	not ready
🔴	01:0079	SIP-Trunk	not ready

Right-click a trunk to display its physical location or to open a trunk line properties window specific to the selected trunk.

Figure 3-5. Trunk View window

The radio button to the left of each trunk location is green when the trunk is idle, and red when the trunk is *not ready* or *in use.* The location format is *logical component ID:channel*—for example, channel 3 on the component in logical component ID 9 is location 09:03. The **Type**, **Status** and **Duration** of trunk use is also displayed.

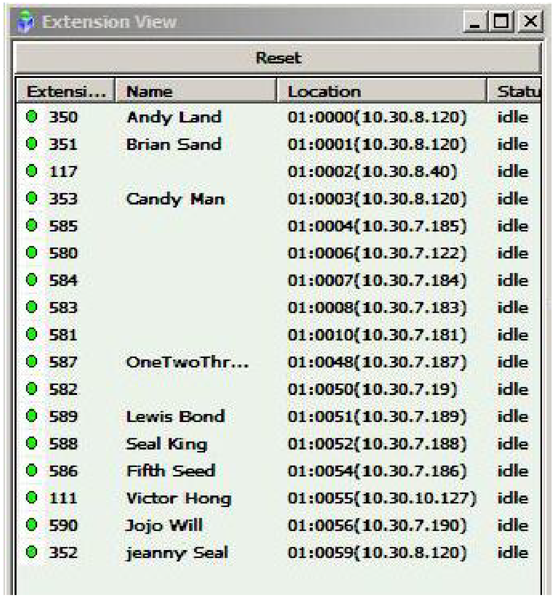
Note: The **Duration** field displays the duration of the trunk only if the call is connected after MaxACD Administrator is started. The field will be empty if the trunk is idle, not ready, out of service, or the call was connected prior to MaxACD Administrator being launched.

You can double-click any trunk location to open the Trunk Configuration window for the selected trunk.

The **Reset** button resets the selected trunk(s) to the idle status if the trunk is connected to a carrier. You'll be asked to confirm the reset, and a status message will tell you if the reset was successful.

Extension View Window

When a Virtual extension registers with the system, it becomes an IP extension and is associated with a SIP Extension channel. Extension view displays the phone's Extension, Name, Location, and Status.

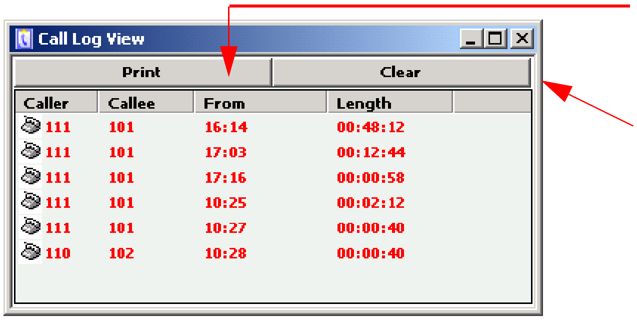


Extensi...	Name	Location	Statu
● 350	Andy Land	01:0000(10.30.8.120)	idle
● 351	Brian Sand	01:0001(10.30.8.120)	idle
● 117		01:0002(10.30.8.40)	idle
● 353	Candy Man	01:0003(10.30.8.120)	idle
● 585		01:0004(10.30.7.185)	idle
● 580		01:0006(10.30.7.122)	idle
● 584		01:0007(10.30.7.184)	idle
● 583		01:0008(10.30.7.183)	idle
● 581		01:0010(10.30.7.181)	idle
● 587	OneTwoThr...	01:0048(10.30.7.187)	idle
● 582		01:0050(10.30.7.19)	idle
● 589	Lewis Bond	01:0051(10.30.7.189)	idle
● 588	Seal King	01:0052(10.30.7.188)	idle
● 586	Fifth Seed	01:0054(10.30.7.186)	idle
● 111	Victor Hong	01:0055(10.30.10.127)	idle
● 590	Jojo Will	01:0056(10.30.7.190)	idle
● 352	jeanny Seal	01:0059(10.30.8.120)	idle

Figure 3-6. Extension View window

Call Log View Window

The **Call Log View** window displays the line and trunk traffic history.



Caller	Callee	From	Length
☎ 111	101	16:14	00:48:12
☎ 111	101	17:03	00:12:44
☎ 111	101	17:16	00:00:58
☎ 111	101	10:25	00:02:12
☎ 111	101	10:27	00:00:40
☎ 110	102	10:28	00:00:40

Prints selected log entries

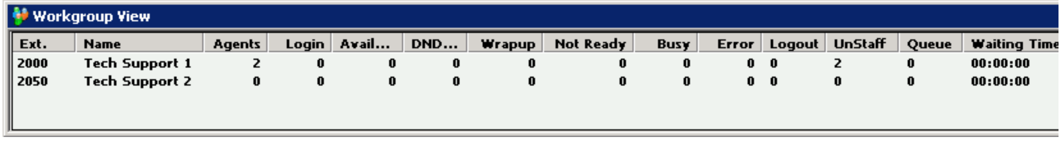
Clears the window of all data

Figure 3-7. Call Log View window

The window displays, for the last 30 calls, the caller line or number, the callee, the starting time in 24-hour format and the length of the call.

Workgroup View Window

The **Workgroup View** window displays data and statistics for workgroups:



Ext.	Name	Agents	Login	Avail...	DND...	Wrapup	Not Ready	Busy	Error	Logout	UnStaff	Queue	Waiting Time
2000	Tech Support 1	2	0	0	0	0	0	0	0	0	2	0	00:00:00
2050	Tech Support 2	0	0	0	0	0	0	0	0	0	0	0	00:00:00

Figure 3-8. Workgroup View window

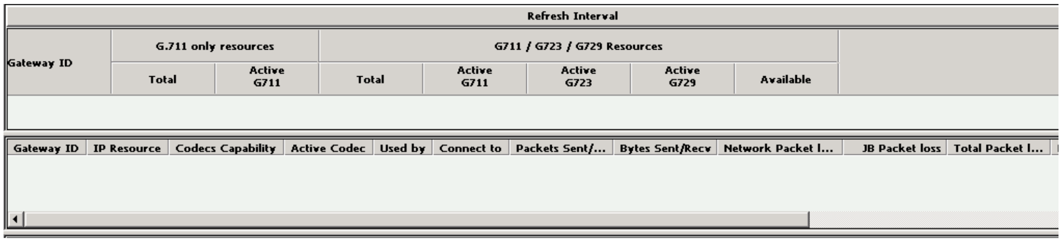
This window displays the following data:

- **Extension**—the workgroup pilot extension number
- **Name**—the workgroup name
- **Agents**—the number of agents assigned to the workgroup
- **Login**—the number of agents logged into the workgroup
- **Available**—the number of logged in agents who are available to receive workgroup calls
- **DND**—the number of logged in agents who are unavailable with the Do Not Disturb status
- **Wrapup**—the number of agents who are in wrapup mode
- **Not Ready**—the number of logged in agents who are in Not Ready state
- **Busy**—the number of logged in agents who are currently on the phone
- **Error**—the number of logged in agents with extensions that are left off-hook or other user error
- **Logout**—the number of agents who are logged out from the workgroup
- **Unstaff**—the number of agents who are logged out from the system
- **Queue**—the number of calls waiting in queue
- **Waiting Time**—the longest wait time of callers in queue
- **Service Level**—the percentage of calls in queue with queue time less than or equal to the defined service level threshold
- **New VM**—new, unread voice mail for the group

Current Resource Statistics Window

The **Current Resource Statistics** window displays the total VoIP channels, available channels, and in-use channels.

The window allows administrators to monitor VoIP channel usage.



Refresh Interval

Gateway ID	G.711 only resources		G711 / G723 / G729 Resources				
	Total	Active G711	Total	Active G711	Active G723	Active G729	Available

Gateway ID	IP Resource	Codecs Capability	Active Codec	Used by	Connect to	Packets Sent/...	Bytes Sent/Recv	Network Packet l...	JB Packet loss	Total Packet l...

Figure 3-9. Current Resource Statistics window

Top part of the window

Contains a summary of resources usage in two categories: **G.71 only** and **G711/ G723/G729**.

Bottom part of the window

Displays the following data:

- **Gateway ID**—the ID of the VoIP channel's home gateway
- **IP Resource**—the VoIP *logical component ID:internal DSP channel ID*
- **Codecs Capability**—the codecs the IP channel can use
- **Active Codec**—the codec currently being used
- **Used By**—the extension, trunk, SIP channel or H.323 channel that is using this channel
- **Connect To**—the extension, trunk, or channel the channel is connected to
- **Packets Sent/Received**—the number of voice packets sent and received
- **Bytes Sent/Received**—the total size (in bytes) of all voice packets sent and received
- **Network Packet Loss**—the number of voice packets that have been lost due to prolonged delays, network congestion, or routing failure
- **JB Packet Loss**—the number of voice packets that have been discarded due to jitter buffer overflow
- **Total Packet Loss Rate**—the ratio of total number of lost packets versus total received packets
- **Max Packet Loss Rate**—the maximum packet loss rate observed over a period of time during a whole session
- **Jitter** —displays the average length of delay per voice packet in milliseconds. This number can be used to measure the quality of service on the network that connects the source and destination sites. Under 100 milliseconds is good, while a higher figure indicates a longer than average delay. (See "Setting VoIP Codec Profiles" on page 191 for more detailed information on jitter.)
- **Local Ports**—displays the local RTP/RTCP port for the voice stream
- **Remote IP Address:Port**—displays the remote RTP port for the voice stream

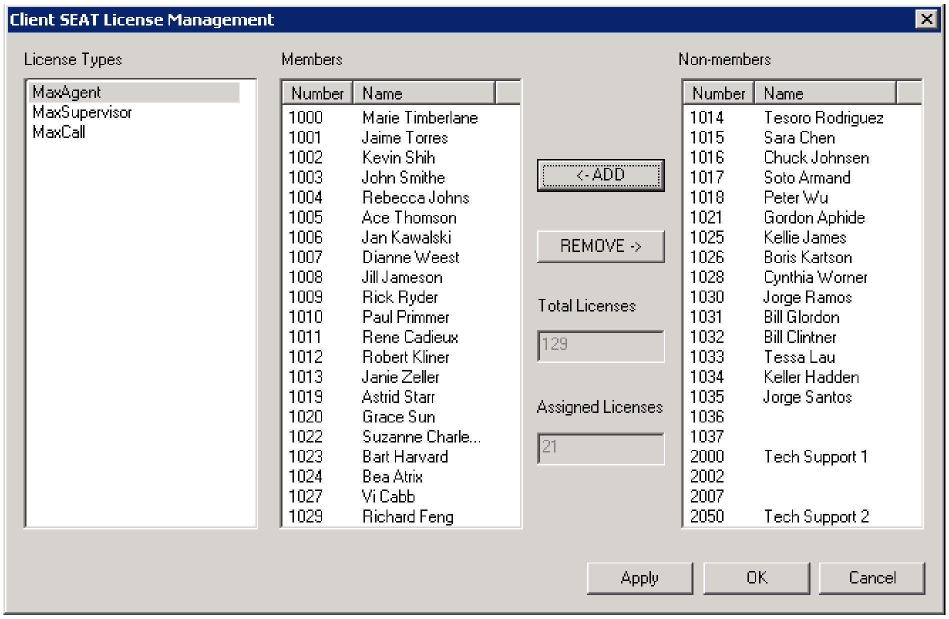
Setting the Refresh Interval

The **Current Resource Statistics** window is updated according to the **Refresh Interval** configuration. By default, the **Refresh Interval** is set to refresh the data in the window every 5 seconds. To change the refresh interval, click the **Refresh Interval** button at the top of the window, and set the refresh interval to a number of seconds up to one minute. Setting the time to 0 is *turning off* the refresh interval.

Assigning Seat-Based Client Licenses

MaxACD for Lync client products require seat-based licenses. If an extension is not assigned to a product, that extension won't be able to use the client product.

Assign extensions to seat-based licenses in the Client SEAT License Management configuration screen (**License > Client SEAT License Management**).



License Types: MaxAgent, MaxSupervisor, MaxCall

Members:

Number	Name
1000	Marie Timberlane
1001	Jaime Torres
1002	Kevin Shih
1003	John Smithe
1004	Rebecca Johns
1005	Ace Thomson
1006	Jan Kawalski
1007	Dianne Weest
1008	Jill Jameson
1009	Rick Ryder
1010	Paul Primmer
1011	Rene Cadieux
1012	Robert Kliner
1013	Janie Zeller
1019	Astrid Starr
1020	Grace Sun
1022	Suzanne Charle...
1023	Bart Harvard
1024	Bea Atrix
1027	Vi Cabb
1029	Richard Feng

Total Licenses: 129

Assigned Licenses: 21

Non-members:

Number	Name
1014	Tesoro Rodriguez
1015	Sara Chen
1016	Chuck Johnsen
1017	Soto Armand
1018	Peter Wu
1021	Gordon Aphide
1025	Kellie James
1026	Boris Kartson
1028	Cynthia Worner
1030	Jorge Ramos
1031	Bill Glordon
1032	Bill Clintner
1033	Tessa Lau
1034	Keller Hadden
1035	Jorge Santos
1036	
1037	
2000	Tech Support 1
2002	
2007	
2050	Tech Support 2

Figure 3-10. Client SEAT License Management dialog box

Select a license type and then select extensions to add to the list of "members" who can use the selected product. Make multiple selections by using Shift+click and Ctrl+click. The screen shows the total number of licenses you have for a client product and the number of licenses assigned.

Stopping the MaxACD Switching Service

Normally, when you exit MaxACD Administrator, the MaxACD services remain active. If you need to shut down the system, from MaxACD Administrator, select **Services > Shut Down All Services**.

This stops the MaxACD system services, including the MaxACD Administrator application itself. When you re-open MaxACD Administrator, the switching services are reactivated.

You can stop MaxACD services only when you are logged in at the MaxACD system computer.

Programs Available from the Windows Start Menu

Several MaxACD programs are available from the Windows **Start** menu.

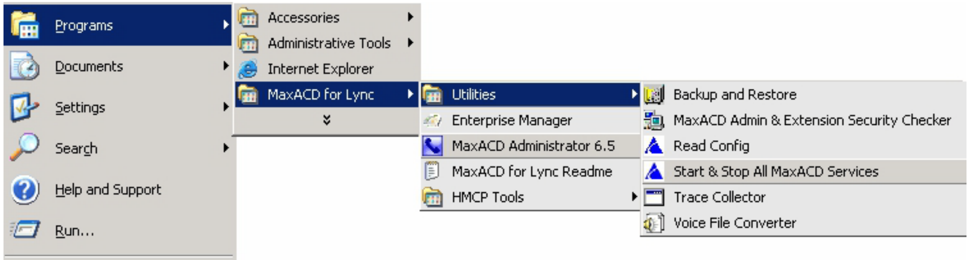


Figure 3-11. MaxACD options on the Windows Start menu

Available under **MaxACD for Lync**:

- **Utilities**—Utilities are described below.
- **Enterprise Manager**—Where you set up the IP dialing table and IP codec profiles. See “Enterprise VoIP Network Management” on page 187. (Available also from MaxACD Administrator.)
- **MaxACD Administrator**—Lets you configure and administer your MaxACD system.
- **MaxACD for Lync Readme**—Readme file for MaxACD for Lync.
- **HMCP Tools**—HMCP Configuration window lets you view some gateway settings and component information and change the ID and password of a gateway. See “Gateway Configuration Tool” on page 81.

Available under **Utilities**:

- **Backup and Restore—**Backs up your configurations and extension voice mail. See “Backup and Restore Utility” on page 225.
- **MaxACD Admin and Extension Security Checker**—Checks the security status of every extension in your MaxACD system. See “MaxACD Admin & Extension Security Checker” on page 228.
- **Read Config**—Creates a subdirectory of HTML files that shows details of your MaxACD configuration. See “Read Config” on page 234.
- **Start and Stop All MaxACD Services**—Opens a dialog box that gives you the option to start or stop all MaxACD services by clicking a button.
- **Trace Collector—**Collects the trace in selected MaxACD categories, within a time range specified, for debugging purposes. See “Trace Collector” on page 231.
- **Voice File Converter**—A voice phrase conversion tool that converts WAV files to ADPCM, WAV to PCM, or ADPCM/PCM to WAV format. See “Voice File Converter” on page 233.

CHAPTER

4

Configuring the MaxACD System

The **System Configuration** window provides for configuring the MaxACD system-wide settings.

To open the System Configuration window, do one of the following:

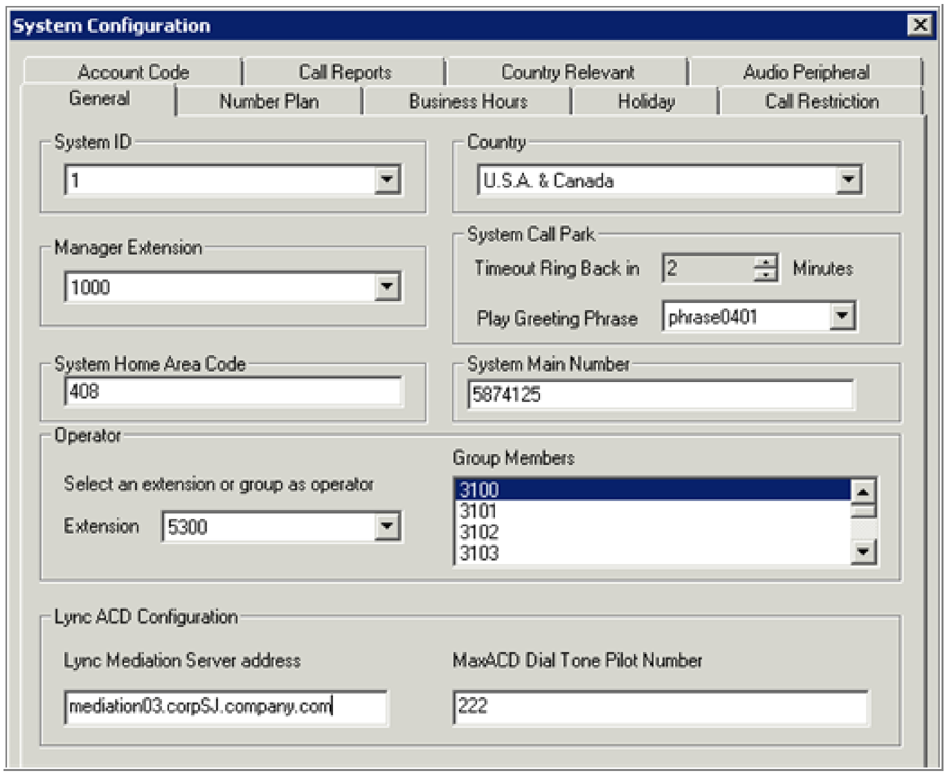
- Click the **System Configuration** button on the toolbar.
- Select **System > System Configuration**.

You can then work with the following settings, each of which is accessed by a tab in the System Configuration window.

- **General setup**—system ID, area code and number, operator and manager extensions, country, system call park options, and Lync ACD configuration.
- **Number Plan**—how the system responds to each first digit dialed
- **Business Hours**—used by system functions
- **Holiday**—how calls are routed on designated holidays
- **Call Restriction**—prefixes to block, toll call prefixes, and call control
- **Account Code**—tables for creating and removing account codes
- **Call Reports**—CDR logging and data export
- **Country Relevant**—settings for toll call prefixes and emergency numbers
- **Audio Peripheral**—settings for music on hold, and system default prompts

Setting General Parameters

Use the **General** tab in the **System Configuration** window to set the system ID and country, home area code and main number, manager and operator extensions, Lync ACD configuration, and options for system call park.



System ID: 1

Country: U.S.A. & Canada

Manager Extension: 1000

System Call Park

Timeout Ring Back in 2 Minutes

Play Greeting Phrase phrase0401

System Home Area Code: 408

System Main Number: 5874125

Operator

Select an extension or group as operator

Extension 5300

Group Members: 3100, 3101, 3102, 3103

Lync ACD Configuration

Lync Mediation Server address: mediation03.corpSJ.company.com

MaxACD Dial Tone Pilot Number: 222

Figure 4-1. System Configuration, General tab

You can set the following parameters and options:

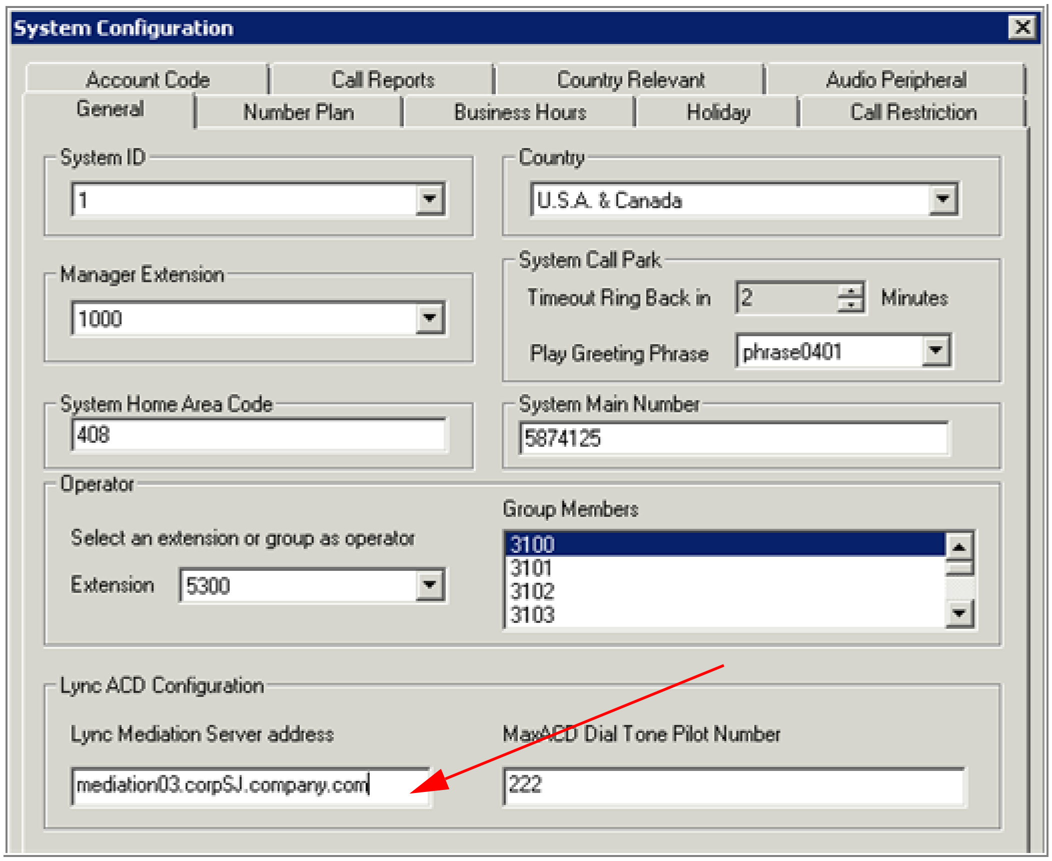
Parameter	Description
System ID	Assign a number (1-100) to the system. This ID will be used to differentiate call records if multiple systems are writing call records to a same external database.
Country	Select a country for the system. This configuration ties to a tone table matched to the country's telecom interface specification.
Manager Extension	Select the system manager’s extension number. The system manager has access to the following system administrator functions: • Record custom phrases • Turn on trunk blocking (#38) • Manage the voice mail’s System Distribution List from the phone

Parameter	Description
System Home Area Code	Area code for the system location. **Note**: This field cannot be blank in the U.S. and Canada.
System Main Number	The main system telephone number. This number will be used as the outbound caller ID in the event that no number is assigned in the trunk Phone Number, 10-digit DID, or extension **Transmitted CID** field. **Note**: This field cannot be blank.
System Call Park • **Timeout, Ring Back in ... Minutes** • **Play Greeting Phrase**	System Call Park (**#41**) allows the extension user to park a call, then pick up the call from another extension. If the call is forgotten, the **Timeout** sets the number of minutes a call remains parked before the user's extension is rung again. To the caller, the call park sounds like being put on hold. Valid entry: 1 - 60 minutes. Select a greeting that the caller will hear before being placed on hold.
Operator Extension and Group Members	Select the extension to be used by the system operator. If the extension number you select is a workgroup, member extensions will show up in the Group Members box. The operator extension is used in the following applications: • Trunk incall routing • DNIS incall routing • Auto Attendant

Configuring Lync Mediation Pool

To configure a Lync mediation pool, use the **General** tab in the **System Configuration** window.

1. On the General tab, enter the DNS name (must be a FQDN) of the Lync Mediation pool.



System ID: 1

Country: U.S.A. & Canada

Manager Extension: 1000

System Call Park
Timeout Ring Back in 2 Minutes
Play Greeting Phrase phrase0401

System Home Area Code: 408

System Main Number: 5874125

Operator
Select an extension or group as operator
Extension 5300

Group Members
3100
3101
3102
3103

Lync ACD Configuration
Lync Mediation Server address: mediation03.corpSJ.company.com
MaxACD Dial Tone Pilot Number: 222

Figure 4-2. Configure Lync Mediation Server address

2. Log onto the Lync Server.
3. Under *Voice Routing*, choose the **Route** tab and configure the IP address of the MaxACD server as a PTSN gateway. If you are using the Redundacy feature, configure two entries: one for the primary server; one for the secondary server.

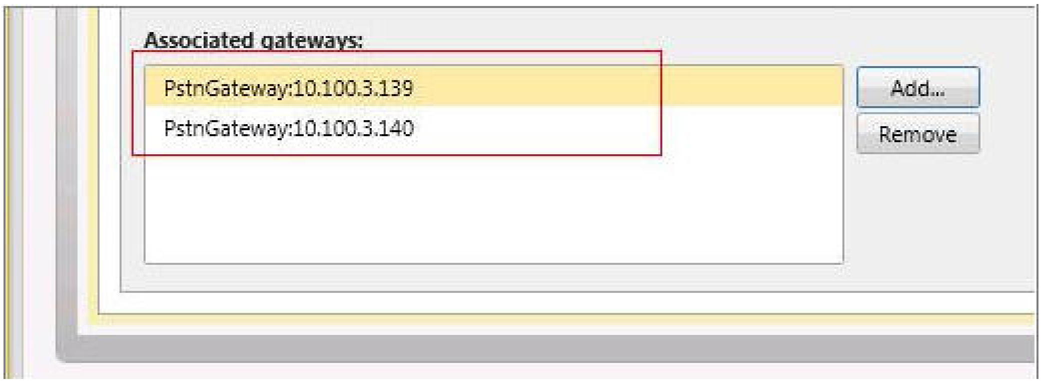
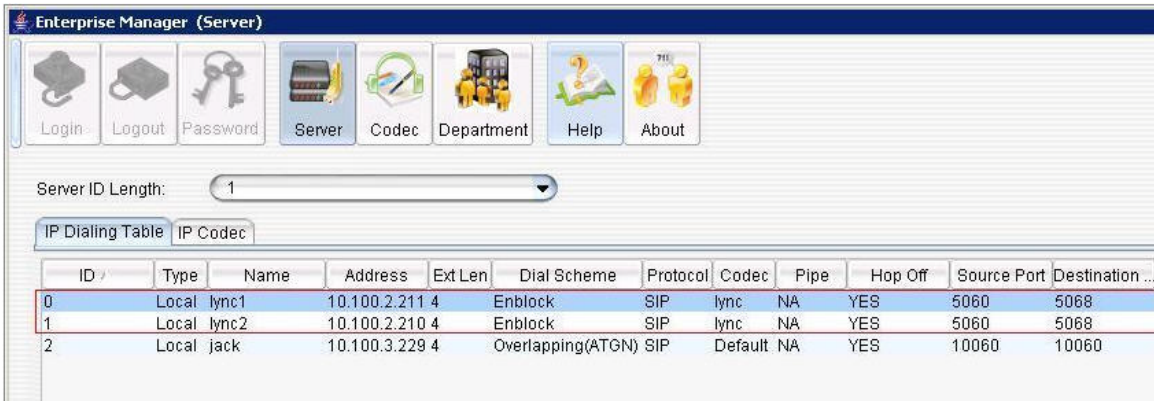

Associated gateways:
PstnGateway:10.100.3.139
PstnGateway:10.100.3.140

Figure 4-3. Lync Server Voice Routing VMGateway configuration

4. Open Enterprise Manager. For each Lync Mediation server, configure the IP dialing entry of the primary and secondary MaxACD server.



Server ID Length: 1

ID	Type	Name	Address	Ext Len	Dial Scheme	Protocol	Codec	Pipe	Hop Off	Source Port	Destination ...
0	Local	lync1	10.100.2.211	4	Enblock	SIP	lync	NA	YES	5060	5068
1	Local	lync2	10.100.2.210	4	Enblock	SIP	lync	NA	YES	5060	5068
2	Local	jack	10.100.3.229	4	Overlapping(ATGN)	SIP	Default	NA	YES	10060	10060

Figure 4-4. Enterprise Manager Server tab

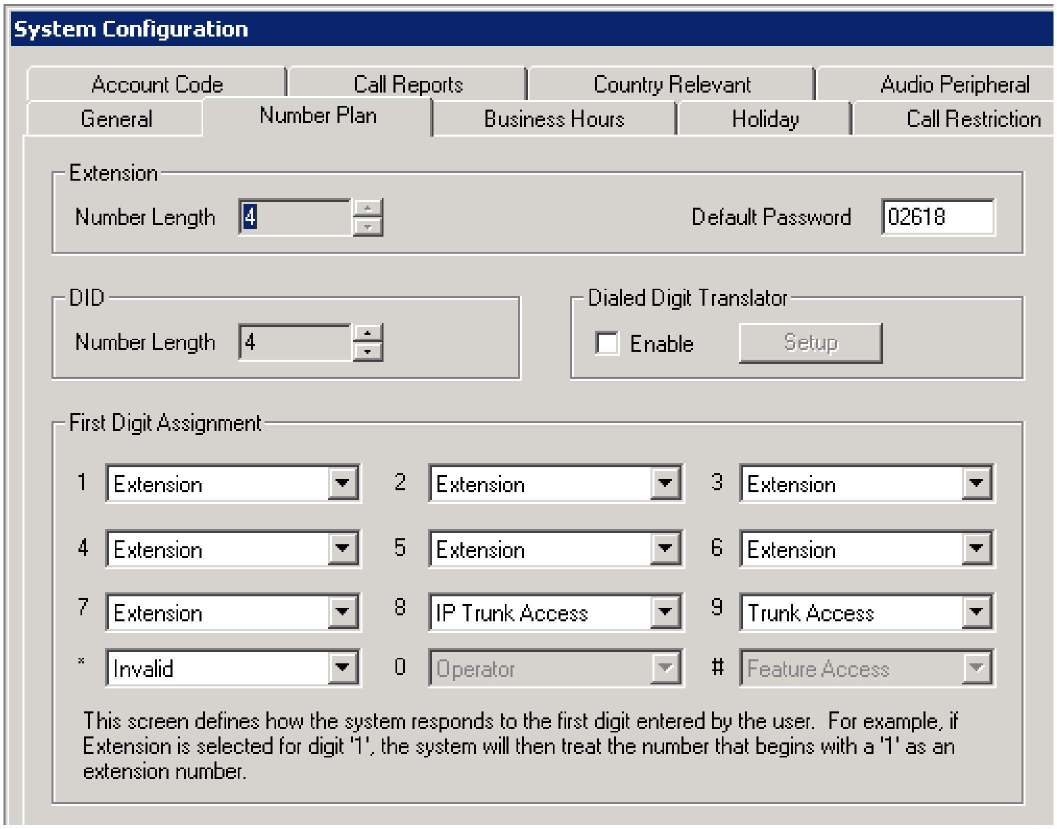
Setting a System Number Plan

The system number plan defines the extension digit length. You can use from 3–6 digits for extensions.

You also set the DID number length and the system response to the first digit dialed—for example, pressing **9** to get a trunk line.

The numbering scheme requires some thoughtful planning.

To set the number plan, select **System > System Configuration**, then click the **Number Plan** tab.



Extension

Number Length: 4

Default Password: 02618

DID

Number Length: 4

Dialed Digit Translator

□ Enable

First Digit Assignment

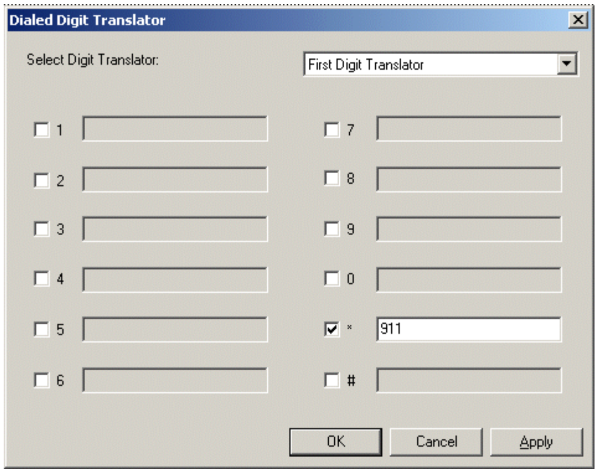
1	Extension	2	Extension	3	Extension
4	Extension	5	Extension	6	Extension
7	Extension	8	IP Trunk Access	9	Trunk Access
*	Invalid	0	Operator	#	Feature Access

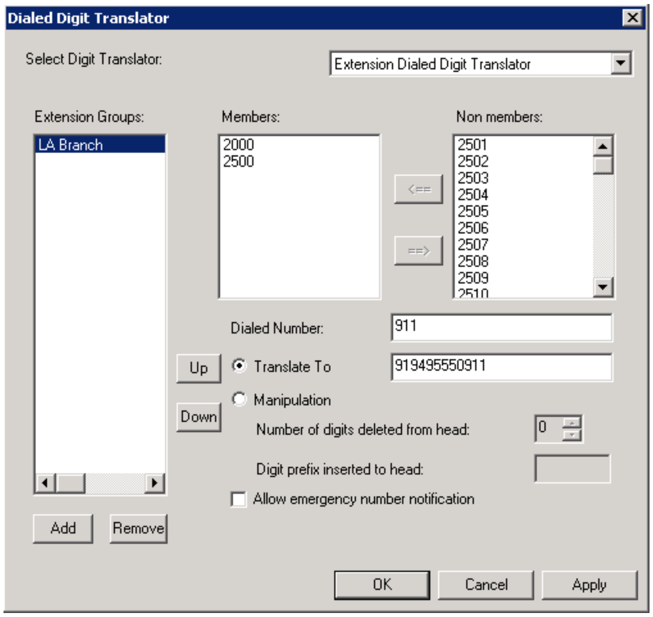
This screen defines how the system responds to the first digit entered by the user. For example, if Extension is selected for digit '1', the system will then treat the number that begins with a '1' as an extension number.

Figure 4-5. System Configuration, Number Plan tab

Use the **Number Plan** tab to specify the following parameters:

Parameter	Description
Extension Number Length	The number of digits for your extension numbering system. Valid entries are from 3–6. For example, extension 2001 and 4020 are 4-digit extension numbers. **Note:** Once the first extension is configured, the extension number length *cannot be changed* without totally reconfiguring the system or deleting all the extensions already configured. Further, if a *first digit dialed* is assigned to extensions and you have set up extensions beginning with that digit, you cannot change the digit assignment without first deleting all affected extensions. For example, if **7** is assigned to *Extension* and you're using extensions 7010, 7113, and so on, you cannot reassign **7** to IP trunk access, without first deleting all the 7*nnn* extensions.
Default Password	The default password for newly created extensions is randomly generated by the system. (When the password is changed, it must be four to eight digits in length.)

Parameter	Description
DID Number Length	The number of digits needed to match a DID (Direct Inward Dialing) number. The range is from 2 - 16. Each extension can be assigned a DID number. A DID number does not have a fixed length. For example, suppose the **DID Number Length** is 4 and the extension DID number is 2522999. Depending on the service contract with the Central Office (CO), the DID trunk can send all 7 digits (2522999) or just the last 4 digits (2999). If the DID Number Length option is set to 4, the system always tries to match the last 4 digits received to the last 4 digits of a DID number, regardless of what is received.
	First Digit Translator Configuration  Dialed Digit Translator Select Digit Translator: First Digit Translator □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 0 ☑ * 911 □ # Figure 4-6. Single Digit Routing To set up a **First Digit Translator** entry, select the check box (to the left of 1-9, * or #), then enter the desired digits. When a box is checked, the digit preprocessor will replace the first digit 1-9, * or # that user dials with the digits indicated in the corresponding field. In the above example, if a user dials "*", the system replaces this with "911". **Note:** This feature is for internal extension users only. It does not support dialing out from voice mail. Improper configuration may cause conflict with the system numbering plan. Be sure to fully test any configuration change in this area before going "live."

Parameter	Description
	Extension Dialed Digit Translator **Note:** This feature is intended for, but not limited to, allowing a remote IP extension to make an emergency call (911) through MaxACD. If MaxACD is in a different location than the IP extension, the emergency call can be routed to the emergency center where the IP extension is located.  Dialed Digit Translator Select Digit Translator: Extension Dialed Digit Translator Extension Groups: LA Branch Members: 2000, 2500 Non members: 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510 Dialed Number: 911 ● Translate To: 919495550911 ○ Manipulation Number of digits deleted from head: 0 Digit prefix inserted to head: □ Allow emergency number notification Up Down <== ==> Add Remove OK Cancel Apply Figure 4-7. Extension Call Routing To set up an Extension Dialed Digit Translator entry: 1. Select **Extension Dialed Digit Translator** from the **Select Digit Translator** drop-down list. 2. In the **Extensions Group** field, use the **Add** button to create and select an extension group that the Extension Dialed Digit Translator will apply to. 3. (optional) From the **Non members** list, you may select an IP extension that the Extension Dialed Digit Translator will apply to. You can apply the same **Members** to multiple locations. You may also enable the **Bypass Account Code** option if Account Codes are required. 4. Enter digits in the **Dialed Number** field and **Translate To** field. In Figure 4-7, assuming the system is located in area code 510, when an IP extension user in LA Branch dials "**911**," MaxACD will translate the digits into "**919495550911**." (9 = IP trunk access code, 19495550911 = the emergency center in LA Branch that covers the remote IP phone user's area.) 5. The **Manipulation** option allows you to remove or add digits to a number dialed by the IP extension. The most common situation requiring this option is to hop-off a VoIP call from a remote system to a remote CO line.

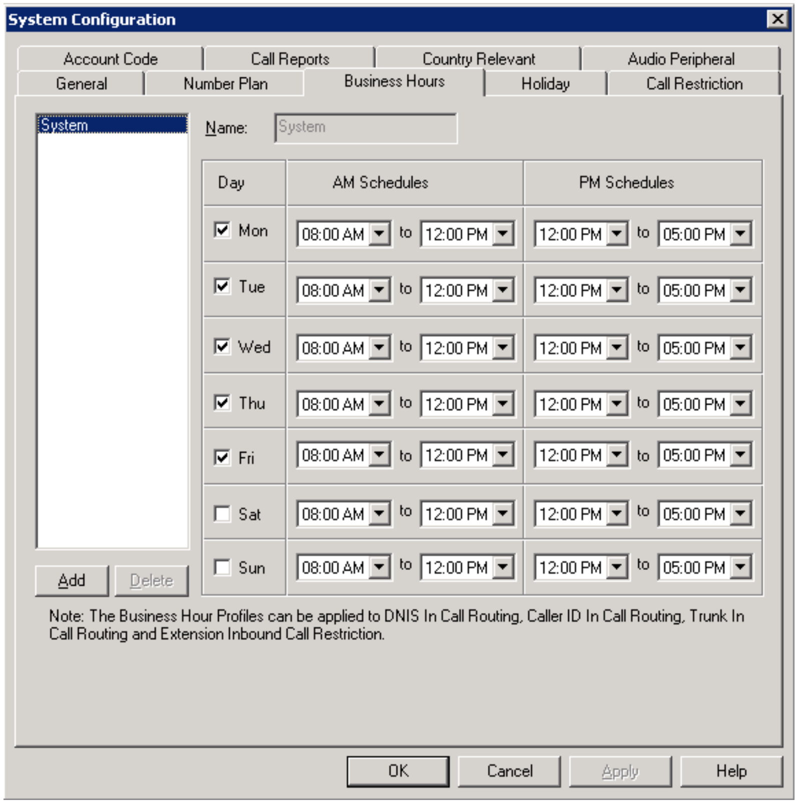
Parameter	**Description**
First Digit Assignment	These define how the system responds to the first digit dialed by the user. The drop-down list options for each digit are: • Extension • Trunk Access • Feature Access • Operator • Invalid (no action) • IP Trunk Access • Route Access **Trunk Access –** Defines how to get a PSTN trunk line to dial an outside number. “9” is the default trunk access code. If you have a more complicated dialing number and routing plan, **change “9” to the Route Access code and configure the Outcall Routing table**. **Feature Access –** By default, **#** is set to Feature Access, which is used as part of feature access codes. In addition, you may also set **1**- **9** or ***** to Feature Access. For example, if **7** is set to Feature Access, Station Login (**#91**) can also be accessed using **791**. Feature access codes are listed in “Feature Access Codes” on page 269. **IP Trunk Access –** Only one IP trunk access option is allowed per system. To use Voice over IP, you must set up this access and, in addition, configure the IP Dialing Table as discussed in “Defining the IP Dialing Table” on page 195 and set the VoIP codecs as discussed in “Setting VoIP Codec Profiles” on page 191. **Route Access –** The Route Access option can be assigned to one or more digits, to route the call per the out call routing table. Out call routing, which is sometimes called ARS (Automatic Route Selection) or LCR (Least Cost Routing without carrier rate table), is described in “Out Call Routing Configuration” on page 115. Out call routing is designed to help 10-digit dialing, Zoomerang dialing, digit manipulation, and tie trunk hop-off dialing.

Setting Business Hours

The Business Hours tab contains group boxes for setting the business hours and days of the week for which the business or organization is in operation. The business hours schedules are used to set other system settings such as trunk, and DNIS and caller ID in-call routing.

Note: Because the business hours are used throughout the system, you or the appropriate administrator must ***make sure the system time has been set correctly***. The system time can be changed using the **Date** and **Time** options in the Windows Control Panel.

To access the Business Hours settings, select **System > System Configuration**, then click the **Business Hours** tab.



Name: System

Day	AM Schedules			PM Schedules		
☑ Mon	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
☑ Tue	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
☑ Wed	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
☑ Thu	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
☑ Fri	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
□ Sat	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
□ Sun	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM

Note: The Business Hour Profiles can be applied to DNIS In Call Routing, Caller ID In Call Routing, Trunk In Call Routing and Extension Inbound Call Restriction.

Figure 4-8. System Configuration, Business Hours tab

Multiple Business Hours profiles can be configured in a system. A default “System” Business Hours profile is already configured. Multiple Business Hours profiles can also be assigned to DNIS Routing and Trunk In Call Routing entries.

To add a Business Hours profile, click the **Add** button. In the **Add Business Hours Profile** dialog box that appears, enter a name for the profile, then click **OK**.

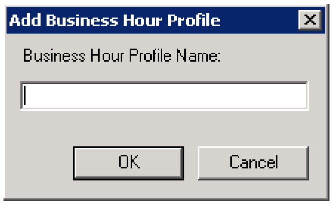


Figure 4-9. Add Business Hours Profile dialog box

For each business hour profile, set the business schedule parameters as follows:

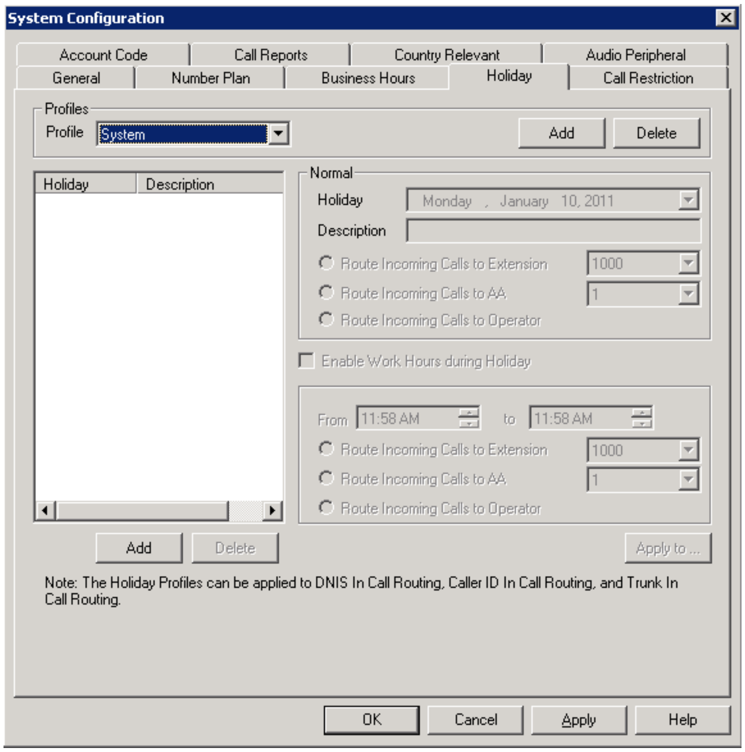
Parameter	Description
Day	Select the days of the week on which the company does business. For example, if the company does business Monday – Friday, check the check boxes for those days.
AM and PM Schedules	For each day of the week, select the time periods during which the company is available for business. The time between the AM and PM times can be used to indicate a lunch break or time between shifts. If you don’t want to set a break between AM and PM schedules, set the PM starting time to be the same as the AM ending time. Or if you want to specify 24 hours as standard business hours, select the following hours: AM Schedules: From 08:00 AM To 12:00PM PM Schedules: From 12:00 PM To 08:00 AM

Routing Calls on Holidays

You can create special routes for incoming DNIS and trunk calls that come in on designated holidays. For holidays that your organization treats as half-days, you can create separate profiles for business and non-business hours.

Note: Incoming DID and tie trunk calls will not follow holiday routes, but go to the dialed extensions directly.

To configure Holiday routings, select **System > System Configuration**, and then click the **Holiday** tab.



Profile: System

Holiday: Monday , January 10, 2011

Description:

○ Route Incoming Calls to Extension 1000

○ Route Incoming Calls to AA 1

○ Route Incoming Calls to Operator

□ Enable Work Hours during Holiday

From 11:58 AM to 11:58 AM

○ Route Incoming Calls to Extension 1000

○ Route Incoming Calls to AA 1

○ Route Incoming Calls to Operator

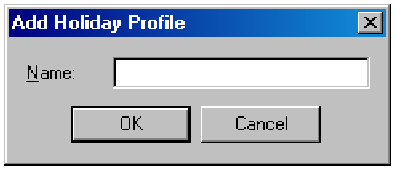
Note: The Holiday Profiles can be applied to DNIS In Call Routing, Caller ID In Call Routing, and Trunk In Call Routing.

Figure 4-10. System Configuration, Holiday tab

Multiple Holiday Profiles can be configured in a system. Each Holiday Profile can include multiple holidays. A default "System" Holiday profile is already configured. Multiple Holiday Profiles can also be assigned to DNIS Routing and Trunk In Call Routing entries.

To create a Holiday Profile

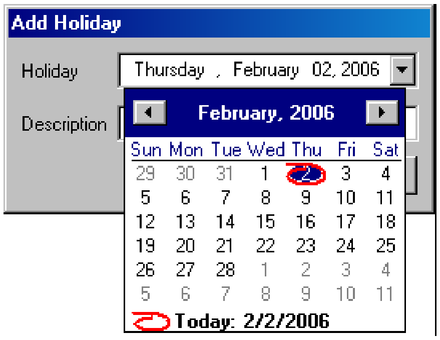
1. Click the **Add** button in the Profiles panel (at the top of the tab) to open the **Add Holiday Profile** dialog box. Enter a name for the profile, then click **OK**.



Name:

Figure 4-11. Add Holiday Profile dialog box

2. To each profile, add holidays that will be included in that profile: Click the **Add** button below the **Holiday** list to create a new holiday.
3. In the **Add Holiday** dialog box that appears, select a date from the drop-down calendar and enter a description to identify the holiday. Click **OK**.



Add Holiday

Holiday Thursday , February 02, 2006

Description

February, 2006

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	1	2	3	4
5	6	7	8	9	10	11

Today: 2/2/2006

Figure 4-12. Add Holiday dialog box

The holiday you added appears in the **Holiday** list. Additional holidays you create appear in the list and together make up the Holiday Profile.

To set call routing

1. Select a Holiday Profile from the **Profile** drop-down list, and then select a holiday in that profile from the **Holiday** list.
2. Set call routing for “normal” holiday hours using the field group in the **Normal** section of the Holiday tab. This will be the default route for calls coming in on that holiday.
3. If you have special work hours during holidays, check the **Special hours** option and configure special hour routing.

   This route will override the route for normal holiday hours, for the hours you specify. Use this option, for example, to route calls for the working portion of a holiday that your organization treats as a half-day.
4. To apply these hours to more than one holiday, click the **Apply To** button and in the **Apply To** dialog box, select all the holidays to which you want the hours to apply. You can select multiple holidays by using **Ctrl-click** or **Shift-click**. Click **OK**.
5. When you are finished with the dialog box, click **OK**.

When a new year begins, the dates on which holidays fall usually change. You can edit the dates for annual holidays, making them accurate for the new year.

To update the date of annual holidays

1. Select a Holiday Profile, and then the holiday from the **Holiday** list. Its date and description appear in the **Normal** section.
2. Click the drop-down arrow beside the date to open a calendar and assign a new date.
3. Click **Apply**.

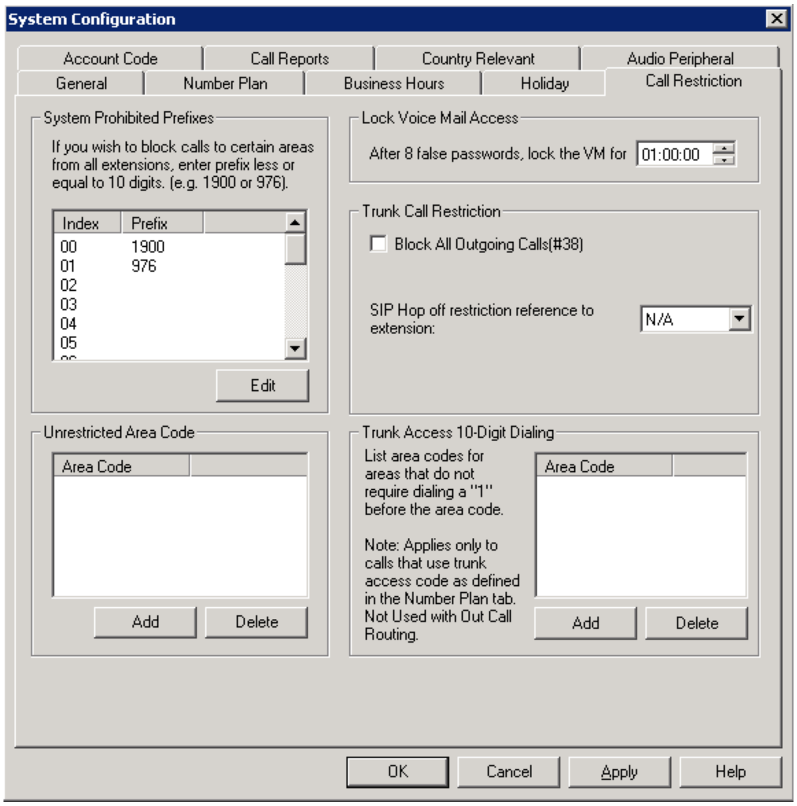
Defining System Call Restrictions

The **Call Restriction** tab contains settings for the following functions:

- Block calls to area codes from all extensions
- Define local/toll-free (unrestricted) area codes
- Lock an attacked extension
- Block all outgoing trunk calls

- Restrict other system users from hopping-off to make an outbound call via a tie trunk
- Set 10-digit dialing area codes for using trunk access code

To set up call restrictions, select **System > System Configuration**, then click the **Call Restriction** tab.



System Prohibited Prefixes

If you wish to block calls to certain areas from all extensions, enter prefix less or equal to 10 digits. (e.g. 1900 or 976).

Index	Prefix
00	1900
01	976
02	
03	
04	
05	

Lock Voice Mail Access

After 8 false passwords, lock the VM for 01:00:00

Trunk Call Restriction

□ Block All Outgoing Calls(#38)

SIP Hop off restriction reference to extension: N/A

Unrestricted Area Code

Area Code

Trunk Access 10-Digit Dialing

List area codes for areas that do not require dialing a "1" before the area code.

Note: Applies only to calls that use trunk access code as defined in the Number Plan tab. Not Used with Out Call Routing.

Area Code

Figure 4-13. System Configuration, Call Restriction tab

Blocking Calls to Area Codes from All Extensions

To add or edit system-prohibited area codes:

1. Double-click an index entry in **System Prohibited Prefixes** list, or select the index entry and click **Edit**. This opens a dialog box that allows you to enter a prefix number.
2. Enter a **1** and the dialing prefix to block (for example, 900, 976). You can enter up to 20 digits maximum for each prefix. For example, to block calls from all extensions to 976 numbers, type 1976.
3. Click **Apply**.

Note: A maximum of 20 prefixes can be defined.

Setting Unrestricted Area Codes

To add or remove “local” call definitions (including calls that begin with 1 but are free: 800, 888), use the **Add** or **Delete** button in the Unrestricted Area Code panel, and click **Apply**. The **Extension Configuration**’s **Restriction** tab references these area codes (as local and unrestricted) in its Outcall Restrictions panel.

Locking Attacked Extensions

If a user enters eight consecutive invalid passwords when logging on to voice mail or to activate an extension, MaxACD considers this an attack. To protect your company from theft of services, you can lock an attacked extension for the period of time you specify (10 minutes - 23 hours, 59 minutes, and 59 seconds) in the **Password Check** field group.

To unlock an extension, use the Extension Checker tool that is installed with MaxACD. See “MaxACD Admin & Extension Security Checker” on page 228.

Blocking All Outgoing Calls

To block all outgoing calls—for example, during the night when no employee is in the office—check the **Block All Outgoing Calls** check box.

Restricting Hop-off Calls

You can set call restrictions on hop-off calls by telling the system to use the same restrictions as the ones set up for an extension. Using the **SIP hop off restriction reference to extension** drop-down list, you can select the extension with the restrictions to use for the hop-off calls.

Setting 10-Digit Dialing Area Codes

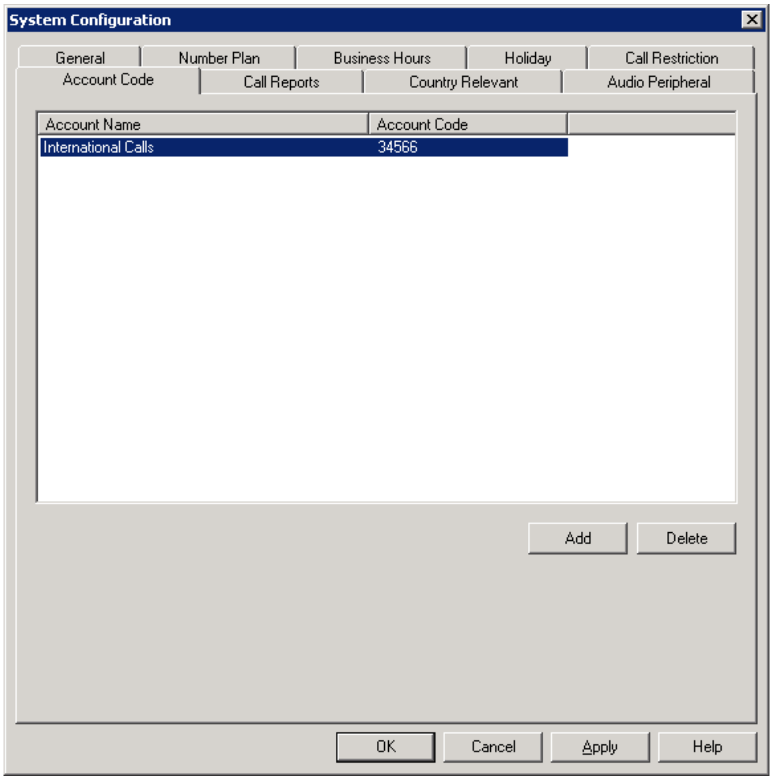
The **10-Digit Dialing Area Code** field lets you define area codes that do not require dialing a “1” before the area code. To enter an area code, click the **Add** button.

Note: Applies only to calls that use a trunk access code. For calls using a route access code, 10-digit dialing area codes need to be configured in the Out Call Routing Configuration window, Dialing Pattern tab. See “Working on Dialing Patterns” on page 119.

Creating Account Codes

Account Codes let you enable or force users to assign incoming and outgoing calls to particular account codes for billing, tracking, or forecasting purposes. Up to 10,000 account codes can be created.

To access the Account Code tab, select **System > System Configuration**, then click the **Account Code** tab.



Account Name	Account Code
International Calls	34566

Figure 4-14. System Configuration, Account Code tab

Adding and Deleting Account Codes

To create an account/code association, click **Add**. Enter an Account Name and Account Code in the dialog box that appears. The Account Code may contain 1-10 digits.

To delete an account and its code, select it and click **Delete**. You can select multiple items for deletion by using **Ctrl-click** or **Shift-click.** Click **Apply** to save your changes and **OK** to save and close the window.

You can now set options for each extension that determine whether account codes must be entered or can be bypassed. You can also block display of the Account Code table (in which case, you would want to supply users with the account codes they need). See "Setting Personal Information" on page 124.

Setting up Call Reports

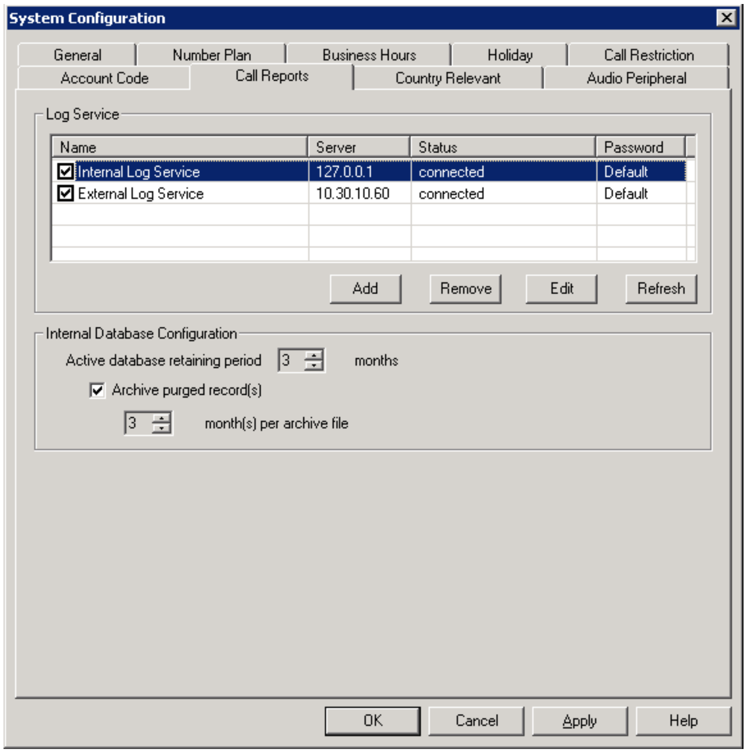
You can set up the call report logging option only if MaxACD and MaxACD Administrator are installed on the same server.

On the **Call Reports** tab, specify the following:

- Where to log the call detail records (CDR). The location can be an internal database, an external database, or both.

- How you want the system to manage an internal CDR database.

To set up Call Reports, select **System > System Configuration**, then click the **Call Reports** tab.



Log Service

Name	Server	Status	Password
☑ Internal Log Service	127.0.0.1	connected	Default
☑ External Log Service	10.30.10.60	connected	Default

Internal Database Configuration

Active database retaining period 3 months

☑ Archive purged record(s)

3 month(s) per archive file

Figure 4-15. System Configuration, Call Reports tab

Internal Database Configuration (Internal Log Service)

The Internal Log Service (shown in the **Log Service** display table) is created by default. You can enable or disable the service, but you cannot remove this database nor add another Internal Log Service.

To manage the internal CDR database:

1. Make sure the **Internal Log Service** check box is checked.
2. In the **Internal Database Configuration** field, use the up/down arrows to select the **Active database retaining period** in months. This determines how long the data will be kept in the database. Valid entry is 1-12 months.
3. (Optional) In the **Archive purged record(s)** field, use the up/down arrows to select the number of months per archive file. This determines the number of months that the system will archive an existing CDR database before creating a new database.
4. Press **OK** or **Apply**.

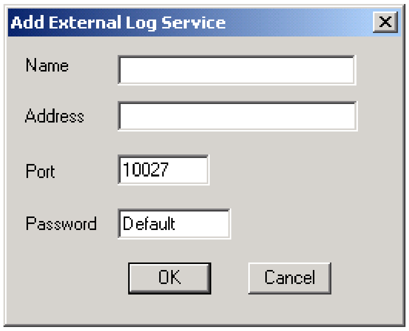
External (Remote) Logging of Call Data

MaxACD allows you to output CDR records to a Microsoft SQL Server database. Before you enable external logging, you need to set up and configure the SQL database and external logger application.

Follow these guidelines:

- The SQL database cannot be on the same server as the MaxACD system. A system integrator or database developer will need to write a custom query to extract data from the SQL database.
- You can send reports from a number of different systems to the same database.
- AltiGen does not provide any SQL backup and restore utility. We strongly recommend that you use SQL Backup and Maintenance utility to perform daily backup and maintenance jobs, and use a restore utility to restore the database. If you need to reconstruct the SQL server, run the External Logger Setup to create an empty calldb database before restore.
- There is no AltiGen license required for external logging.

To set up and enable external CDR login service to the local or network drive, click **Add**.



Port: 10027

Password: Default

Figure 4-16.   Add External Log Service

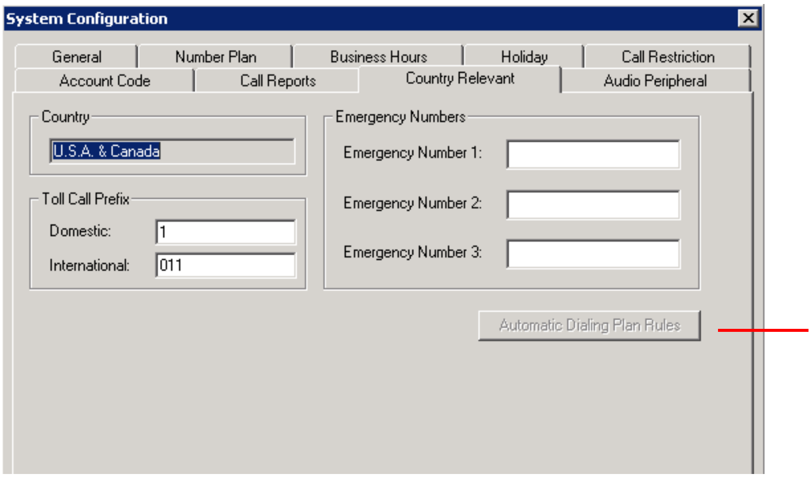
Fill in the fields, and click **OK**.

Parameter	Description
Name	The name of the external log service machine (optional)
Address	The IP address of the external log service machine
Port	The TCP port of the machine
Password	The password to connect to the external service machine

Country-Relevant Settings

The **Country Relevant** tab in the **System Configuration** window contains group boxes for setting toll call prefixes and emergency numbers.

The **Country** field displays the country selected on the System Configuration, **General** tab.



Country: U.S.A. & Canada

Toll Call Prefix

Domestic: 1

International: 011

Emergency Numbers

Emergency Number 1:

Emergency Number 2:

Emergency Number 3:

If your system is not in North America, The **Automatic Dialing Plan Rules** button is available.

Figure 4-17. System Configuration, Country Relevant tab

Setting Toll Call Prefixes

MaxACD uses **Toll Call Prefixes** to determine the type of outside call and imposes restrictions when necessary. For example, if the international toll call prefix is **011** and a user attempts to make an international call from an extension without international call privileges, the call will be terminated as soon as the user dials **011** after the trunk or route access number. The caller hears an error tone.

The toll prefixes set here should match the dialing plan prefixes for the country set in the **General** tab (see “Setting General Parameters” on page 32). You can set the following toll call prefixes.

- **Domestic**. The dialing plan for your country’s domestic long distance prefix. For example, type in a **1** for 1-plus dialing within the U.S. dialing plan (also known as the North American Numbering Plan).
- **International**. The prefix used for international calls. For example, this is **011** for international calls made in the U.S.

Setting Emergency Numbers

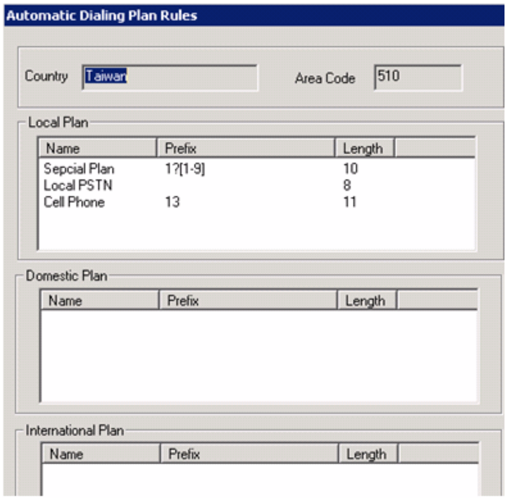
The number in the **Emergency Number** field will have the system automatically find a trunk to process the call without the extension user dialing a trunk access code first. You may enter up to three emergency numbers in the appropriate fields.

Note: This feature works with both trunk access code and route access code.

Dialing Plan Rules for Non-North American Country

If your MaxACD system is in a country other than the U.S.A. or Canada, you can configure a call return rule based on the country, which will greatly improve the call return feature from Caller ID, Zoomerang, and making a call from Microsoft Outlook.

Click the **Automatic Dialing Plan Rules** button.



Country: Taiwan

Area Code: 510

Local Plan

Name	Prefix	Length
Sepcial Plan	1?[1-9]	10
Local PSTN		8
Cell Phone	13	11

Domestic Plan

Name	Prefix	Length

International Plan

Name	Prefix	Length

Figure 4-18.   Automatic Dialing Plan Rules dialog box

Define the Local Plan, Domestic Plan, and International Plan. A character of the pattern can be a digit from 0 to 9. It can also be a range of digits, for example, [0-3]. If it is a question mark, '?', it is equivalent to [0-9].

When return calls are made, these rules are followed:

- When the number matches Local Plan, the system will send the number out to the trunk directly.
- When the number matches the Domestic Plan, the system will send the number out with the domestic toll call prefix.
- When the number matches the International Plan, the system will send the number out with the international toll call prefix.

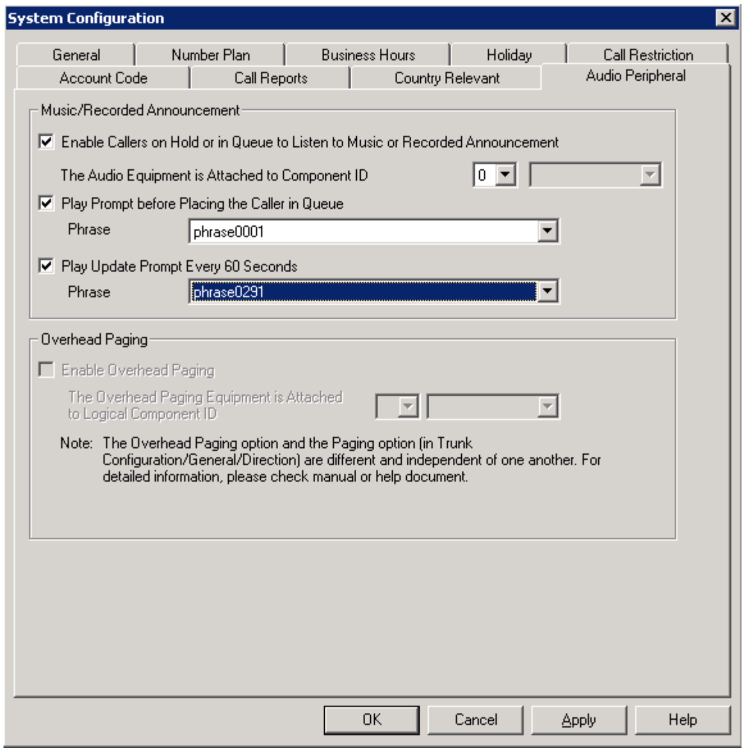
When a number matches multiple entries, the match with the most digits has priority.

Audio Peripheral Configuration

You can configure audio peripheral settings:

- Music on hold
- System default beginning and update prompts for callers in queue

To access the **Audio Peripheral** configuration window, select **System > System Configuration**, then click the **Audio Peripheral** tab.



Music/Recorded Announcement

☑ Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement

The Audio Equipment is Attached to Component ID: 0

☑ Play Prompt before Placing the Caller in Queue

Phrase: phrase0001

☑ Play Update Prompt Every 60 Seconds

Phrase: phrase0291

Overhead Paging

□ Enable Overhead Paging

The Overhead Paging Equipment is Attached to Logical Component ID

Note: The Overhead Paging option and the Paging option (in Trunk Configuration/General/Direction) are different and independent of one another. For detailed information, please check manual or help document.

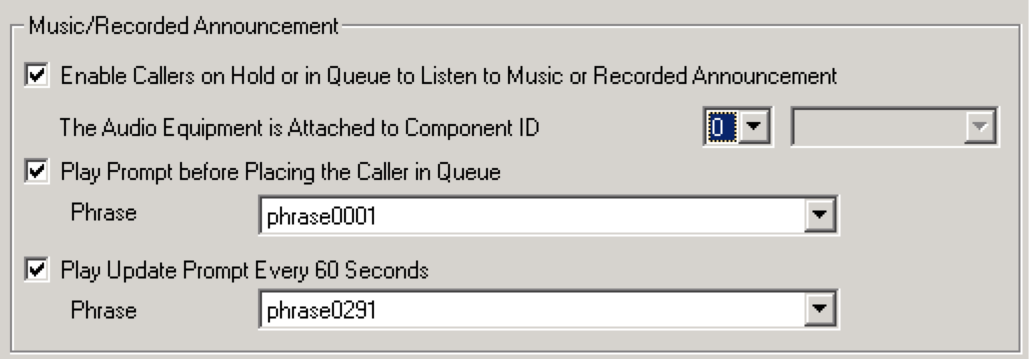
Figure 4-19. System Configuration, Audio Peripheral tab

Configuring Music On Hold and Recorded Announcements

Callers will hear the music or recorded announcement configured on this tab *only* if the user places the caller on hold.

To configure music on hold when using audio equipment

1. Check **Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement**.
2. Select the component ID to which the audio equipment is attached.



Music/Recorded Announcement

☑ Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement

The Audio Equipment is Attached to Component ID: 0

☑ Play Prompt before Placing the Caller in Queue

Phrase: phrase0001

☑ Play Update Prompt Every 60 Seconds

Phrase: phrase0291

Figure 4-20. Music/Recorded Announcement dialog box

To configure music on hold to play a file

1. Check **Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement**.
2. Use the drop-down list to select the component ID.

   The system will play the default music-on-hold file when the user places the caller on hold.

The default music-on-hold file is a .wav file called "MusicOnWaiting.wav". The file is located in the C:\PostOffice\phrases\Music folder. You can replace the file with a .wav file (or an AltiGen PCM file). The .wav file must be in 8 kHz/ 8 bit/ Mono/ u-Law format. Any optional music-on-hold files included with MaxACD are in that format. You can convert your own .wav files to this format using Microsoft Windows Sound Recorder.

Note: You may need to reduce the music volume level 70-80% to avoid distortion.

To replace the default music-on-hold file

1. Back up the default file.
2. On the **Audio Peripheral** tab, clear the **Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement** check box.
3. Rename the desired .wav file to "MusicOnWaiting.wav" and put it in the C:\PostOffice\phrases\Music folder.
4. On the **Audio Peripheral** tab, check the **Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement** check box.

Note: If you have two files named MusicOnWaiting in the MusicOnWaiting folder, one a .wav file and one a PCM file, the .wav file takes precedence.

Setting Greeting and Update Prompts

To play a prompt before placing the caller into a hold queue:

1. Select the **Play Prompt Before Placing the Caller in Queue** check box.
2. Use the drop-down list to select the prompt number you want to use for the greeting message. (Creating prompts is discussed in "Phrase Management" on page 72.)

To play an update prompt every 60 seconds:

1. Check the **Play Update Prompt Every 60 Seconds** check box.
2. Use the drop-down list to select the prompt number you want to use for the greeting message.

Note: These settings will be used by all workgroups as the default system queue phrase. However, these settings will be overridden by the workgroup's queue management phrase setting.

CHAPTER

5

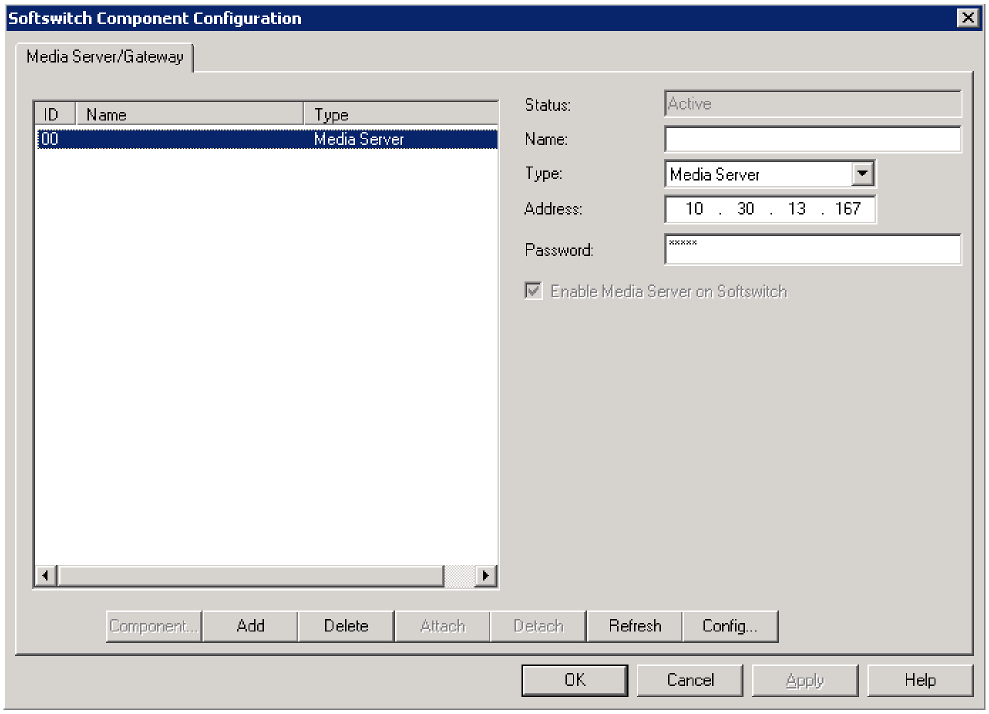
Media Server Management

When MaxACD and HMCP media server are installed in different machines, you will perform media server management functions in the Softswitch Component Configuration window.

The Softswitch Component Configuration window lists each media server in your system, its ID, name, and type, status, IP address, password. Use this window to:

- Add and delete a media server
- Attach and detach a media server
- Change a media server name, IP address, password, country
- Enable media server on the MaxACD machine

To open the Softswitch Component Configuration window, select **System > Softswitch Component Management**.



Softswitch Component Configuration

Media Server/Gateway

ID	Name	Type
00		Media Server

Status: Active

Name:

Type: Media Server

Address: 10 . 30 . 13 . 167

Password: *****

☑ Enable Media Server on Softswitch

Figure 5-1. Softswitch Component Configuration window, Media Server/Gateway tab

Setting Parameters

To read or set parameters for a media server, first select the media server in the list on the left and make your changes, and then click **OK**.

Parameter	Description
ID/Name/Type	Lists media servers that have been added using the **Add** button in this window.
Status	Shows the status of the selected media server: active, disconnected, initializing, resetting, failed. (Read-only field.)
Name	The name you gave the selected media server for easy identification.
Type	Shows whether this is a media server or gateway. If the ID is other than 00, you cannot change the type in this configuration screen. If you want to change the type, you need to delete the entry and recreate it.
Address	The IP address of the selected media server.
Password	The password assigned to the selected media server. (Each media server has its own password.)
Refresh button	Refreshes the selected media server’s (read-only) status display
Config button	Opens the AltiGateway Configuration Tool, where you can see information on the selected media server and change the ID and password for this media server.

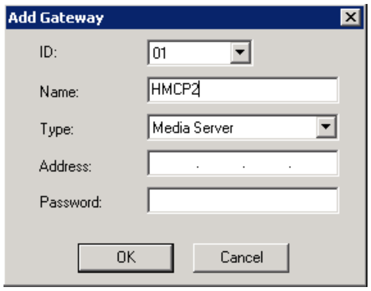
Adding and Attaching a Media Server

Caution! Always try to attach a media server when call activity in the system is low. If resources are being used in one of the media servers, ***ongoing calls may be dropped*.**

To attach a media server to the MaxACD system, you must first add it to the list in the Softswitch Component Configuration window.

To add a media server to the list:

1. Click the **Add** button.



ID: 01

Name: HMCP2

Type: Media Server

Address: . . .

Password:

Figure 5-2. Add Gateway dialog box

2. Set this media server unique number. Each media server in the system must have a unique identifying number.
3. Specify a name for the media server that identifies it to you.
4. Select the type: **Media Server**.
5. Enter the IP address of the media server.
6. Create a password for this media server. The password is used for access to the Gateway Configuration Tool for the media server.

After you add a media server to the list, you can attach it to the MaxACD system. Also, you may have disconnected a media server that has already been attached. In either case, you can attach it in the Softswitch Component Configuration window.

To attach a media server to the MaxACD system:

1. Select the media server you want to attach.
2. Click the **Attach** button.

   It takes 2-5 minutes to attach a media server. If a “Failed” message appears, you may have entered an incorrect IP address or password, or the media server may already be attached.

Detaching and Deleting a Media Server

You can detach a media server without shutting down the MaxACD system.

Caution! Always try to detach a media server **when call activity in the system is low**. If resources are being used in one of the media servers, ***ongoing calls may be dropped***.

To detach a media server from the MaxACD system:

1. Select the media server you want to detach.
2. Click the **Detach** button. You are asked for confirmation.
3. Click **Yes** to confirm. A message appears telling you that the detachment was successful, and the **Status** field of the media server reads **Disconnected**.

To delete a media server from the Softswitch Component Configuration window:

First detach the media server. Then select the media server you want to delete, and click the **Delete** button. The media server disappears from the window. You can add it back again, if you want, by using the **Add** button.

Changing Media Server ID and Password

You can change the selected media server's unique number (01, 02) and the password by clicking the **Config** button in the Softswitch Component Configuration window. This opens the Gateway Configuration Tool. Make your changes, and click **Apply**.

HMCP Configuration Tool

The configuration tool that opens when you click the **Config** button in the Softswitch Component Configuration window can also be opened from the **Start > All Programs > MaxACD > HMPC Tools > HMPC Configuration**. When you open it from the **Start** menu, you'll see this dialog box:

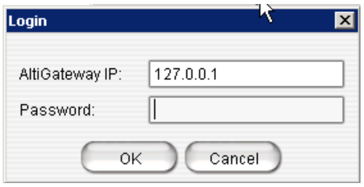
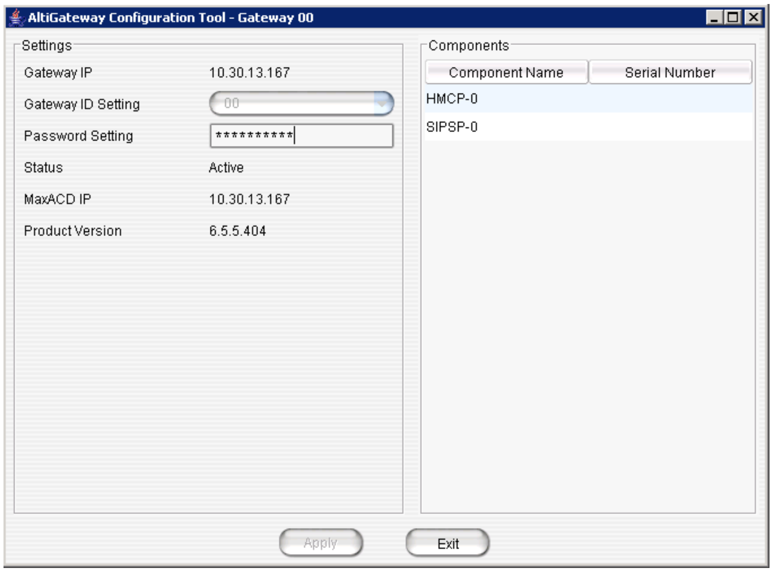


Figure 5-3. HMCP Configuration Tool log-in dialog box

Enter the IP address and password of the media server you want to check on, and click **OK**.

The HMCP Configuration Tool looks like this:


AltiGateway Configuration Tool - Gateway 00

Settings

Gateway IP 10.30.13.167

Gateway ID Setting 00

Password Setting **********

Status Active

MaxACD IP 10.30.13.167

Product Version 6.5.5.404

Components

Component Name	Serial Number
HMCP-0	
SIPSP-0	

Figure 5-4. HMCP Configuration Tool

The window displays media server settings, product version, and a component view for the media server, showing each component name and serial number.

The settings:

Parameter	Description
Gateway IP	The IP address of the media server identified in the title bar.
Gateway ID Setting	Shows the unique numeric ID of the media server identified in the title bar. (Editable field.)
Password Setting	The password of the media server identified in the title bar. (Editable field.)
Status	The status of the media server: active, disconnected, initializing, resetting, failed.
MaxACD IP Address	The IP address of the machine running MaxACD.
Product Version	The software version of the media server service.

Figure 5-5. Softswitch Component Configuration window, **Applications Server** tab

CHAPTER

6

Voice Mail Configuration

Use the **Voice Mail Configuration** window to control the following:

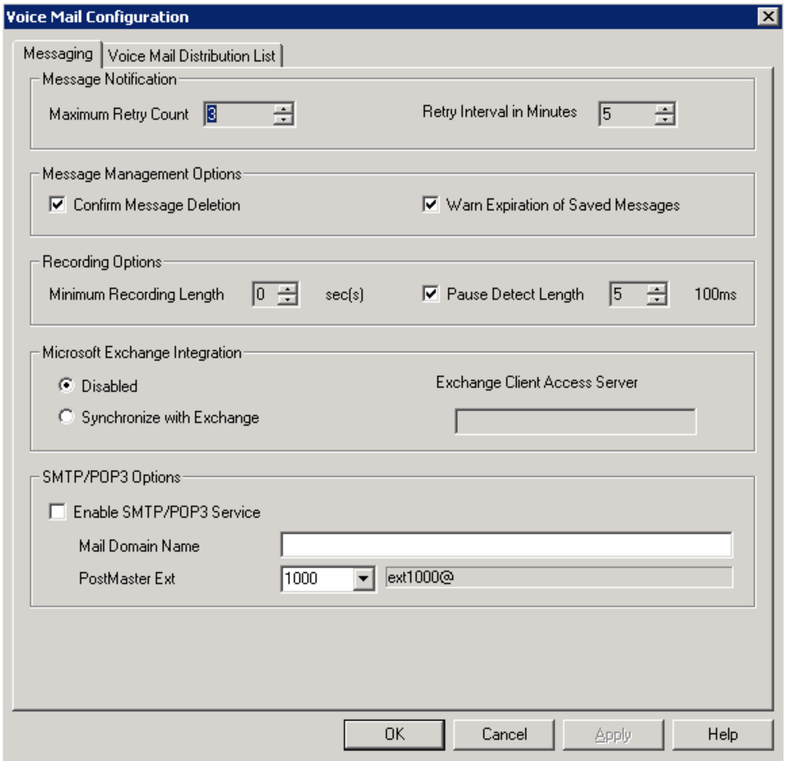
- How the system processes voice mail notification
- How the system processes voice mail deletion and expired messages
- How the system records voice mail, system phrases, custom phrases, personal greetings, directory name recording, and queue phrases
- Enable or disable SMTP/POP3 service to deliver voice mail to an e-mail address as an attachment
- Enable or disable Microsoft Exchange synchronization service

To access the Voice Mail Configuration window, do one of the following:

- Select **System > Voice Mail Configuration**
- Use the drop-down list beside the **System** button, and select **Voice Mail Configuration**.

Managing Messages

The **Messaging** tab in the Voice Mail Configuration window provides for setting basic parameters and options for messaging, including message notification retry attempts, message management options, recording options, and e-mail activation and usage.



Message Notification

Maximum Retry Count 3

Retry Interval in Minutes 5

Message Management Options

☑ Confirm Message Deletion

☑ Warn Expiration of Saved Messages

Recording Options

Minimum Recording Length 0 sec(s)

☑ Pause Detect Length 5 100ms

Microsoft Exchange Integration

● Disabled

○ Synchronize with Exchange

Exchange Client Access Server

SMTP/POP3 Options

□ Enable SMTP/POP3 Service

Mail Domain Name

PostMaster Ext 1000 ext1000@

Figure 6-1. Voice Mail Configuration, Messaging tab

Setting Message Notification Retries

When a message is sent to a user's voice mailbox and outcall notification is configured, the system will try to call a phone number, pager, or an extension to deliver notification. You can set the retry setting for the notification as follows:

Parameter	Description
Maximum Retry Count	Can be between **0** and **16**. This is the number of times the system will try to deliver a voice message notification *after* the original attempt. For example, **5** retries means five tries after the original, or 6 total attempts.
Retry Interval in Minutes	The number of **minutes** between retry attempts. Five minutes is the minimum and 60 minutes is the maximum interval allowed. Choices are in 5-minute increments. The default is 5 minutes.

Setting Message Management Options

Set voice mail message confirmation and warning parameters:

Parameter	Description
Confirm Message Deletion	If checked, the system plays a voice message instructing the user to confirm request for deletion by pressing the # key. This prevents users from accidentally deleting messages with a single key entry.
Warn Expiration of Saved Messages	If checked, the system warns the user that saved messages will be deleted due to their retention time expiring. The message is given the day before the messages are automatically deleted, and the user then has the option to either keep or delete the messages. By default, this feature is enabled. **Note:** If this feature is disabled, saved messages are deleted automatically without warning when they expire.

Setting Message Recording Options

Set voice mail message recording parameters:

Parameter	Description
Minimum Recording Length	Sets the minimum length in seconds for any recording (incoming voice mail message, personal greeting, system prompts, introductions to forwarded voice mails). This can be from 1–5 seconds, or 0, which means no minimum. All recordings that are shorter than the designated Minimum Recording length are deleted. This feature is recommended when users receive many short, empty voice mail messages on a regular basis and would like them automatically deleted.
Pause Detect Length	Selected, this feature causes the deletion of pauses in messages. The default pause detect length is **500 ms**. The pause detect can be disabled by deselecting the check box, or the length can be set to a value between **200–2000 ms (.2–2 seconds)**.

Setting the Exchange Integration Option

Access to the Exchange integration option requires an AltiGen Exchange Integration License. To assign this license to an extension, see “Assign Exchange Integration License” on page 130.

You may choose the option when you install MaxACD, and you may change the option later. If you change the option later, you need to restart services.

Parameter	Description
Disabled	Disables Exchange integration.

Parameter	Description
Synchronize with Exchange	Allows a two-way synchronization between a user's MaxACD voice mail and the user’s Outlook-readable mail messages with their attached .wav files in the user's inbox. When e-mails or voice mails are deleted from one server, they are automatically deleted from the other server as well. If you select this option, enter the DNS name of the Exchange server in the **Exchange Client Access Server** field (do *not* enter the IP address).

Setting E-mail Messaging Options

To use the MaxACD e-mail services, configure the following settings.

Parameter	Description
Enable SMTP/ POP3 Service	Selected, this enables incoming and outgoing mail services on MaxACD—Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3).
Postmaster Ext	This field defines the extension that will be assigned as a Postmaster Extension. When the e-mail system receives an e-mail with an invalid e-mail account, the automatic reply to the sender (informing of the invalid e-mail account used) is sent from the defined extension. **Note:** The system always requires an extension to be specified as the Postmaster Extension. By default, the first extension in the system is used. If an extension is selected as the Postmaster Extension, it cannot be deleted until the Postmaster Extension is re-assigned to another extension.

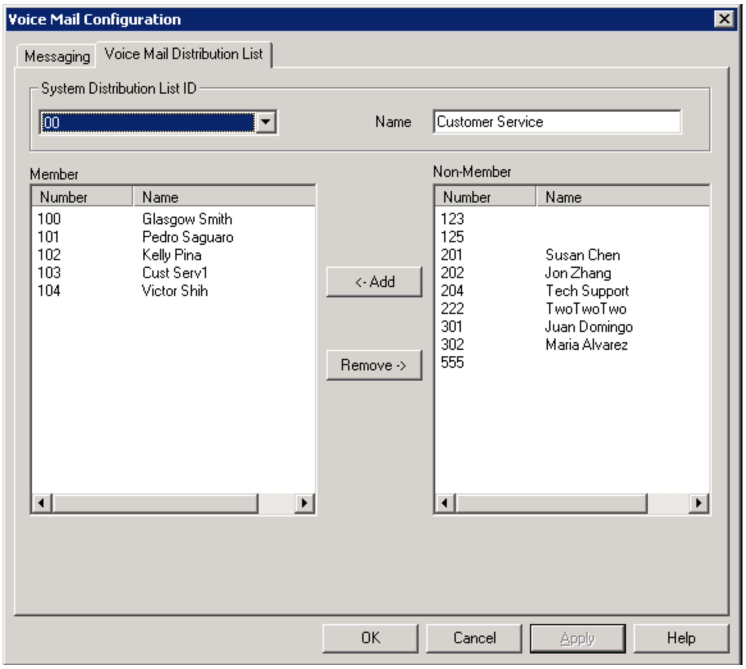
Creating Distribution Lists

The System Distribution Lists provide for forwarding voice mail messages to multiple recipients defined as list members. To forward a voice mail to all list members, a user needs to enter only the two-digit ID instead of entering numerous individual extensions.

You can create up to 100 distribution lists, each composed of up to 64 extensions. The extension list member can represent another distribution list.

Note: The *system* distribution lists discussed here are different from the *extension* distribution lists, which are configured through the phone sets or the MaxAgent for Lync user application.

To configure distribution lists, select **System > Voice Mail Configuration**, then click the **Voice Mail Distribution List** tab.



System Distribution List ID: 00

Name: Customer Service

Member

Number	Name
100	Glasgow Smith
101	Pedro Saguaro
102	Kelly Pina
103	Cust Serv1
104	Victor Shih

Non-Member

Number	Name
123	
125	
201	Susan Chen
202	Jon Zhang
204	Tech Support
222	TwoTwoTwo
301	Juan Domingo
302	Maria Alvarez
555	

Figure 6-2. Voice Mail Configuration, Voice Mail Distribution List tab

Defining a Distribution List

1. On the Voice Mail Distribution List tab, select an ID (00 – 99) in the **System Distribution List ID** drop-down list.

   The list name, if any, now appears in the **Name** box; the members of the list are now displayed in the **Member** box, and other available extensions are displayed in the **Non-Member** box.

2. To give the list a name or change the existing name, type a descriptive name into the **Name** box.

3. To *add* a member, select the name(s) in the **Non-Member** list and click the **Add** button to move it to the **Member** list.

   To *remove* a member, select the name(s) in the **Member** list and click the **Remove** button to move it to the **Non-Member** list.

   You can select multiple names by using **Shift**-click or **Ctrl**-click.

4. Click **Apply** to save your changes, or click **OK** to save and close the Voice Mail Configuration window.

CHAPTER

7

Auto Attendant Configuration

The auto attendant (AA) feature provides quick and courteous processing of all incoming calls. An AA can be configured to serve as a primary attendant or as a backup to a receptionist. In a call-heavy environment the AA can greatly reduce the number of calls that need to be handled by the operator.

You can set up to 255 different AAs. AA features include:

- Multiple levels of tree structure.
- Repeat current level or jump to a specific level.
- Transfer call to extension, workgroup, hunt group, or operator.
- Dial by Name—allows a caller who does not know the extension number to spell the name using the telephone key pad. The system will search the Directory and make a match on the name to connect the caller to the intended party's extension.
- Name Directory Service—allows callers to hear a list of employees and their extension numbers.
- Records a voice mail message to a specific mail box.
- Allows employees to call into the system and access voice from an external location.
- Collects caller input data, for example, account code, ID, and so on.
- Data-Directed Routing—Allows the routing of calls directed by the caller's input (digit or text).
- Sets call priority and skill level requirement for workgroup call processing.
- Other advanced features include System Call Back and routing calls to SDK-based add-on applications.

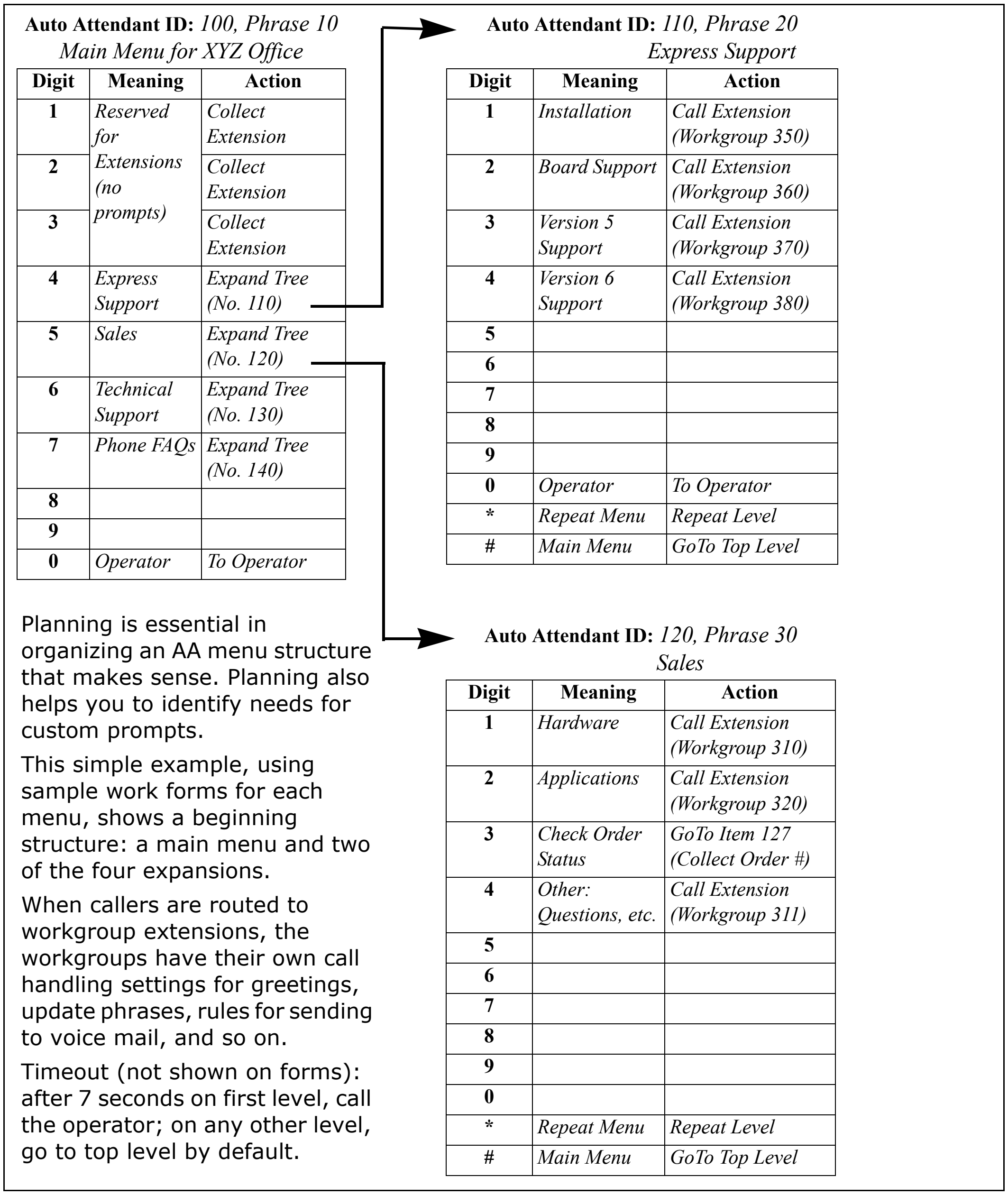
Planning Is Essential

Follow the steps below before you set up an AA.

1. Before you configure tasks for one or more AAs, you should plan the entire setup. Decide how many options you will provide at each menu and how many menu levels you will use. Based on the action choices in each menu, write down the appropriate prompts or phrases that are to be played at each menu level.
2. Record phrases for each menu level or use the pre-recorded phrases that are available to you. See “Phrase Management” on page 72 for more details on how to

record custom phrases, use pre-recorded phrases and use professionally recorded phrases.

Example: AA Planning



Auto Attendant ID: *100, Phrase 10*
Main Menu for XYZ Office

Digit	Meaning	Action
1	*Reserved for Extensions (no prompts)*	*Collect Extension*
2		*Collect Extension*
3		*Collect Extension*
4	*Express Support*	*Expand Tree (No. 110)*
5	*Sales*	*Expand Tree (No. 120)*
6	*Technical Support*	*Expand Tree (No. 130)*
7	*Phone FAQs*	*Expand Tree (No. 140)*
8		
9		
0	*Operator*	*To Operator*

Auto Attendant ID: *110, Phrase 20*
Express Support

Digit	Meaning	Action
1	*Installation*	*Call Extension (Workgroup 350)*
2	*Board Support*	*Call Extension (Workgroup 360)*
3	*Version 5 Support*	*Call Extension (Workgroup 370)*
4	*Version 6 Support*	*Call Extension (Workgroup 380)*
5		
6		
7		
8		
9		
0	*Operator*	*To Operator*
*	*Repeat Menu*	*Repeat Level*
#	*Main Menu*	*GoTo Top Level*

Planning is essential in organizing an AA menu structure that makes sense. Planning also helps you to identify needs for custom prompts.

This simple example, using sample work forms for each menu, shows a beginning structure: a main menu and two of the four expansions.

When callers are routed to workgroup extensions, the workgroups have their own call handling settings for greetings, update phrases, rules for sending to voice mail, and so on.

Timeout (not shown on forms): after 7 seconds on first level, call the operator; on any other level, go to top level by default.

Auto Attendant ID: *120, Phrase 30*
Sales

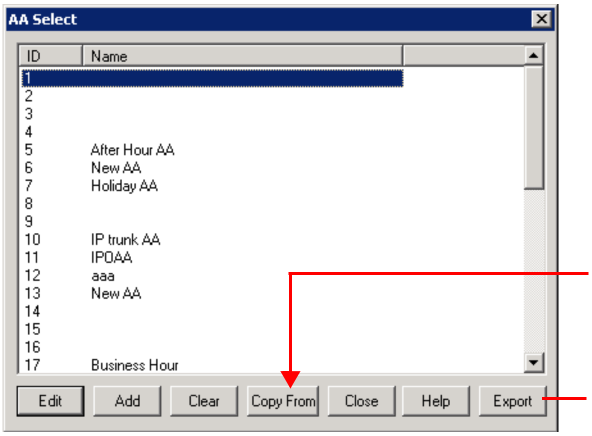
Digit	Meaning	Action
1	*Hardware*	*Call Extension (Workgroup 310)*
2	*Applications*	*Call Extension (Workgroup 320)*
3	*Check Order Status*	*GoTo Item 127 (Collect Order #)*
4	*Other: Questions, etc.*	*Call Extension (Workgroup 311)*
5		
6		
7		
8		
9		
0		
*	*Repeat Menu*	*Repeat Level*
#	*Main Menu*	*GoTo Top Level*

Adding Auto Attendants

The first 16 AAs are provided with the menus blank. You can edit these as described in “Configuringing Auto Attendants” on page 68. You don’t need to add a new AA if you’re going to use 16 or fewer.

To add an AA beyond the first 16:

Click the **AA Configuration** button, or select **System > AA Configuration**.



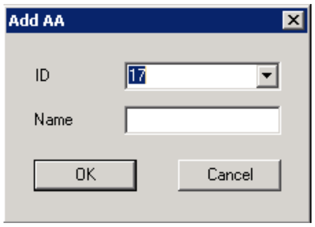
ID	Name
1	
2	
3	
4	
5	After Hour AA
6	New AA
7	Holiday AA
8	
9	
10	IP trunk AA
11	IPOAA
12	aaa
13	New AA
14	
15	
16	
17	Business Hour

Copies an AA to a selected ID.

Exports all your AA settings to an HTML file

Figure 7-1. AA Select window

- **Edit**—opens the AA window, where you can edit the selected AA as described in “Configuringing Auto Attendants” on page 68.
- **Add**—opens the Add AA dialog box.



ID 17

Name

Figure 7-2. Add AA dialog box

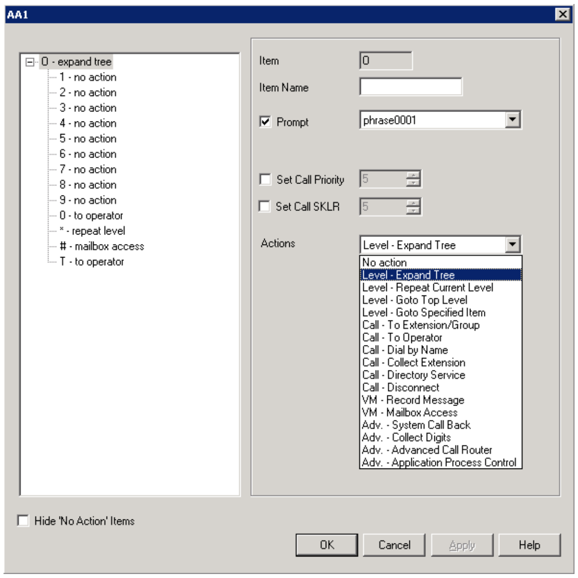
Select an **ID** in the drop-down list and type in a descriptive **Name** for the AA, then click **OK**.

- **Clear**—clears all edits to the selected AA, restoring system defaults.
- **Copy From**—lets you make a copy of an AA (and then modify it, as you like).
  1. Select your target ID from the AA Select window.
  2. Click the **Copy From** button.
  3. From the drop-down list, choose the AA you want to copy to your selected ID.
  4. In the pop-up box, click **Yes** to complete the copy.
- **Close**—closes the AA Select dialog box.
- **Help**—opens the help file for AA.
- **Export**—exports all AA settings to an HTML file.

Configuringing Auto Attendants

To configure an AA, click the **AA Configuration** button, or select **System > AA Configuration**. In the window, select an AA in the list and click **Edit**.

This opens the **AA** window, showing the AA you selected in the title bar.



AA1

- O - expand tree
  - 1 - no action
  - 2 - no action
  - 3 - no action
  - 4 - no action
  - 5 - no action
  - 6 - no action
  - 7 - no action
  - 8 - no action
  - 9 - no action
  - 0 - to operator
  - * - repeat level
  - # - mailbox access
  - T - to operator

Item: O

Item Name:

☑ Prompt: phrase0001

☐ Set Call Priority: 5

☐ Set Call SKLR: 5

Actions: Level - Expand Tree

☐ Hide 'No Action' Items

Figure 7-3. AA window

Note: You can check the **Hide 'No Action' Items** check box to hide items that are set to "no action." This will give you a cleaner view of your various action items.

Configuring Menu Items

The AA is a tree-based structure with unlimited tree levels. The following rules guide the basic AA configuration:

- Each item is an action point with its ID number and name.
- The top of the tree is a "O" (for Origin).
- A timeout is indicated by a "T".
- Any action item can have a "Prompt". The drop-down list displays phrase files located at C:\Postoffice\Phrases\LangCustom directory. A phrase file can be any file name.
- If one action item has multiple choices, you need to select "Expand Tree" instead of using "Go to next menu" to create a new level.
- You can jump to any action item within the same AA.

Every item will execute steps according to the following rules:

- First step—Play prompt if the box is checked. If the prompt box is not checked, the AA will go to the second step without delay.

- Third step—Set Call Priority for MaxACD priority queuing. You can assign a priority number from 1-9 to the caller who selects this menu item. The highest priority is 1, the lowest priority is 9. If this box is not checked, go to the next step without delay.
- Fourth step—Set Call SKLR (Skill Level Requirement) for MaxACD skill-based routing. You can assign an SKLR from 1-9 to the caller who selects this menu item. If this box is not checked, go to the next step without delay.
- Fifth step—Execute the action selected from the drop down list. The drop down list contains the following actions:

Action	Description
No Action	An "invalid" message plays and the menu is repeated.
Level - Expand Tree	Expand menu item to create additional level.
Level - Repeat Current Level	Repeats the level that contains the "Repeat Current Level" menu item.
Level - Go to Top Level	Go to the top level and repeat action items on the top level.
Level - Go to Specified Item	Goes to selected menu item at any level. A drop-down list appears from which you select the item.
Call - To Ext./ Group	Transfers call to an extension or group number you select in the drop-down list.
Call - To Operator	Routes the call to the operator (the operator is defined in the System Configuration window).
Call - Dial By Name	Prompts the caller to enter the name (first, or last, or both in any order) of the person they want to speak with and dials the extension that matches the name. Callers may not have to enter the entire first or last name before a match is found.
Call - Collect Extension	The top level of each AA collects the extension number automatically. The system has a timing delay to differentiate if the first digit the caller entered is a menu option or the first digit of an extension number. Once past the top level, the system will not have the timing delay to differentiate digits. If you would like to provide the option for a caller to enter an extension number, you need to map this action item to one of the menu options.
Call - Directory Service	Lists the system users and their extensions to the caller. For this to work properly, users need to record their directory names.
Call - Disconnect	Disconnects the call.
VM - Record Message	Leaves a voice mail message in the specified voice mail box. If you want the caller to hear the extension's greeting before hearing the start-recording beep, check **Play Extension Greeting**.
VM - Mailbox Access	Allows the caller to log in to the voice mail system to retrieve voice mail or change personal options from the outside. This option is assigned to the "#" key at the top level of each AA by default.

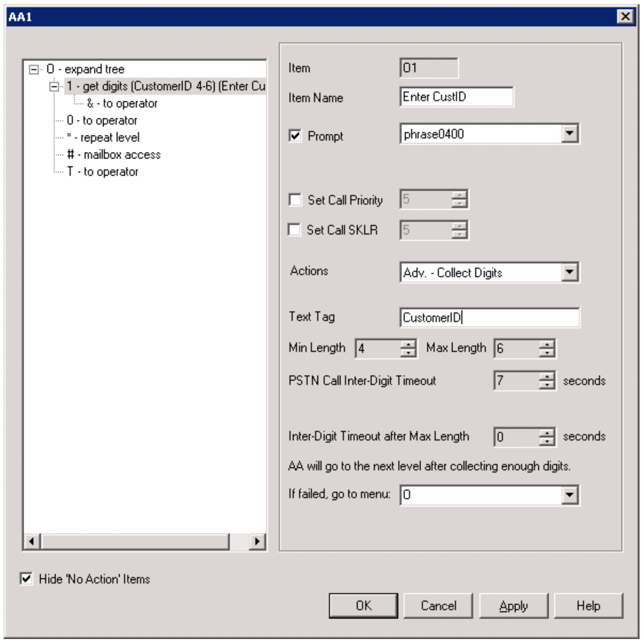
Action	Description
Adv. - System Call Back	Allows outside caller to dial into the system, enter a call back number, hang up, and wait for the system to call back. The system will request the caller to enter an extension and password for authentication. The call back number needs to include the toll call prefix and area code for long distance and international calls. The trunk or route access code is not required when entering a call back number.
Adv. - Collect Digits	See the discussion below on "Collecting Digits".
Adv. - Advanced Call Router	When selected, the system will hand over the call to the Advanced Call Router application through the SDK API interface. The ACR application needs to log in to a virtual extension with the correct password. If the ACR application fails to connect, the system will execute the sub-level "&" as a fail action.
Adv. - Application Process Control	When selected, the system will hand over the call to the APC (Application Process Control) SDK through an application extension as a control extension. An SDK APC based application needs to log in to the application extension to receive the call. If the APC application fails to connect, the system will execute the sub-level "&" as a fail action.

Collecting Digits

When a caller selects the "Collect Digits" action item, a custom phrase is required to advise the caller how many digits are required. The system will look at "Min Length" and "Max Length" to determine if the collect digit action was successful or failed.

- If successful, the system executes the sub-level "&" action item.
- If failed, the system executes the menu item you define as a fail over action.

To use the Collect Digits action, select the **Adv. - Collect Digits** action, then set the following additional parameters:



- 0 - expand tree
  - 1 - get digits (CustomerID 4-6) (Enter Cu
    - & - to operator
  - 0 - to operator
  - * - repeat level
  - # - mailbox access
  - T - to operator

Item: 01

Item Name: Enter CustID

☑ Prompt: phrase0400

□ Set Call Priority: 5

□ Set Call SKLR: 5

Actions: Adv. - Collect Digits

Text Tag: CustomerID

Min Length: 4 Max Length: 6

PSTN Call Inter-Digit Timeout: 7 seconds

Inter-Digit Timeout after Max Length: 0 seconds

AA will go to the next level after collecting enough digits.

If failed, go to menu: 0

☑ Hide 'No Action' Items

Figure 7-4. Collect digits dialog box

- **Text Tag**—a tag name, which is critical for the following operations:
  - For CDR logging, the **IVRData** field will log the collected digits as "Tag=xxxxx". For example, if tag is configured as "Account" and collected digits is "67663", the CDR database will log "`Account=67663`" in the **IVRData** field.
  - For MaxAgent client display, the above example is displayed as "Account=67663" on the **View > IVRData** section.
  - To display collected digits on the IP phone, you need to set the tag as "DISP" (stands for "Display" and is case-sensitive. The **Phone Display/Name Line** of the extension configuration needs to be configured as **IVR Data (Display)**. This feature supports inbound trunk calls only.
- **Min. Length**—the *minimum* length of digits to be collected.
- **Max. Length**—the *maximum* length of digits to be collected.
- **PSTN Call Inter-Digit Timeout**—the length of time the system will wait between collecting of digits before timing out.
- **Inter-Digit Timeout after Max Length**—the length of time the system will wait after the maximum length of digits is collected.

Making Auto Attendant Assignments

Once the AAs are set up, you can use them in various in-call routing situations—trunk, DNIS, caller ID, in-call routing, and an answering option for an extension or workgroup.

For example, for trunk /AA assignments, see “Incoming Call Routing” on page 106. For extension or group assignments, see “Setting Answering Options” on page 138.

Phrase Management

You might want to record unique phrases to customize an AA or a group. When the system is configured to have the AA answer incoming calls, callers hear a customized greeting. For example:

> “Thank you for calling ABC Company.
> Enter the extension number of the person you wish to speak with.
> Press 1 for sales.
> Press 2 for technical support.
> Press 3 for accounts payable.
> Press 0 to reach the operator.
> To repeat this menu, press star (*).”

An example of a group greeting phrase:

> “Please hold; someone will be with you shortly.”

You might also want to give callers the option of hearing prompts in another language. For information on configuring for a multilingual AA, see “Multilingual Configuration” on page 75.

This section covers information on how to use pre-recorded phrases, record custom phrases, and use professionally recorded phrases.

Using Pre-Recorded Prompts

MaxACD provides ready-to-use pre-recorded phrases. Phrase 0001 is the default AA greeting at the root menu level. Phrases 0291 through 0297 are phrases used for group queue prompts. Select the phrase you want to use in the **Prompt** field. To hear the pre-recorded phrases:

1. Use any phone to dial “###”, and log in with the system manager’s extension and password.
2. Press 6 for the Phrase Management option.
3. Press 1 to review a phrase.
4. Enter the 4-digit phrase number from the list below to hear the phrase.

Phrase #	Phrase
0001 **(default)**	Thank you for calling. If you know the extension of the person you wish to speak with, please enter it now. To reach the operator, press **0** or simply stay on the line.
0291 **(default)**	Please hold; someone will be with you shortly. For your convenience, you may leave a message if you wish by pressing the # key on your telephone and we will get right back to you.
0292	Please hold; someone will be with you shortly.
0293	We appreciate your call and will be with you as quickly as possible.
0294	Thank you for your patience. We should be with you soon.
0295	Thank you for your patience. We should be with you soon. For your convenience, you may leave a message if you wish by pressing the # key on your telephone and we will get right back to you.
0296	We apologize for the extended delay, but our current call load is abnormally high. Remember, you may leave a message by pressing the # key on your telephone and we will get right back to you.

Phrase #	Phrase
0297	You may still wait if you prefer, but we suggest you leave a message by pressing the # key on your telephone and we will get right back to you.

Using Professionally Recorded Phrases

Recording studios such as Worldly Voices provide professionally recorded prompts as electronic files that can be installed and used on the MaxACD system. (See the AltiGen web site, at **www.altigen.com**, for more information. Click **Customer** at the top of the page, and then click **Resources for Creating Professional Voice Prompts**.)

AltiGen provides the Voice File Converter utility to convert these files into the proper MaxACD format (available from the Windows **Start > Programs > MaxACD for Lync > Utilities** menu). Some recording studios provide the conversion service for an additional fee. The converted file can then be used for an AA or for a workgroup setup.

To install professionally recorded phrases or prompts:

1. Assign a prompt number to each prompt you would like recorded. Or give the prompt a unique identifying name. MaxACD-supplied phrases are numbered, but phrases don’t have to be numbered.
2. Submit your prompt script and prompt name to the recording studio.
3. Instruct the recording studio to record prompts in either 8KHz or 11.025KHz mono in the WAV format.
4. Ask the studio to convert the WAV file(s) into the proper MaxACD format.
   - If using Worldly Voices, this conversion is done for you.
   - If you are using a studio other than Worldly Voices, use the Voice File Conversion utility. This utility converts an audio file recorded at either 8KHz or 11.025KHz in the WAV format to an MaxACD playable audio file.
5. Once you receive the prompts in the MaxACD format, place them in the **C:\PostOffice\phrases\LangCustom** directory on the server that is running MaxACD.

Your prompts are now ready to be used.

CHAPTER

8

Multilingual Configuration

MaxACD supports multiple language prompts (8 languages total) for trunk calls and extension users, letting you configure your system to handle the following types of scenarios in a multilingual environment:

- An auto attendant (AA) may serve callers who speak different languages. MaxACD can be configured to let the caller select a preferred language in which to hear prompts. Once a language is selected, the whole call session will use the selected language.
- An internal user may use a feature code to execute a certain action, including logging into voice mail. Normally the user hears system prompts first. If the user is not fluent in the default system language, another language can be assigned to his extension. Whenever that extension user encounters prompts, the system will use the assigned language to play the prompts.
- DNIS may also be used to select a language for the caller. If your company has multiple phone numbers, you can configure MaxACD to direct a caller to a language based on the phone number the caller has dialed. For example, if you give out different 800 numbers to different countries, and a call comes in from the 800 number you give out to customers in Mexico, you can configure MaxACD to direct that 800 number to the "Mexico Spanish" language prompts or to an extension that uses the corresponding language in its prompts. This eliminates the caller having to select a language.

Note: The MaxACD multilingual feature requires the purchase of an AltiGen Multilingual License.

Configuration Overview

Configuring multilingual features involves most or all of the following actions, which are discussed in subsequent sections:

- Have the appropriate system and custom phrases recorded in each language that your company wants to use (in addition to the default language).
- Store the custom phrases in new directories under the C:\PostOffice\Phrases directory, using the prescribed naming convention.
- Add the new languages to the Multilingual Configuration screen.
- Enable auto attendant support in the Multilingual Configuration screen, AA tab.

- In the Extension Configuration screen, choose an available language for the internal user, if desired.
- Enable the extension user to change the preferred language for the extension by using feature code **#12**, if desired.
- Configure the **Language Setting** in DNIS, if desired.

Creating Language Phrase Packages

For each set of phrases you want in a different language, you need to have phrases recorded in that language. See "Using Professionally Recorded Phrases" on page 73 for details. Each language's phrase package must contain phrase files, and two text files: one text file that lists syntax rules for numbers, and one that lists syntax rules for sentence structure, since these vary from language to language.

The phrase files will have the exact same name/number as in the default language directory and will be part of the same AA, but they will be stored in a different directory.

Storing Language Phrase Packages

Additional language phrases (system and custom) and syntax styles need to be copied to the correct directory before system startup, so that the system can recognize them. If they are added *after* system startup, MaxACD needs to be shut down and restarted, before the directories are recognized.

The next figure illustrates the directory storage structure for language phrases.

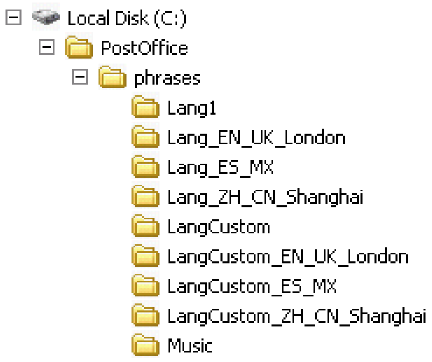


Figure 8-1. Storage structure for multilingual phrases

The directories `Lang1` and `LangCustom` contain the phrases of the system default language.

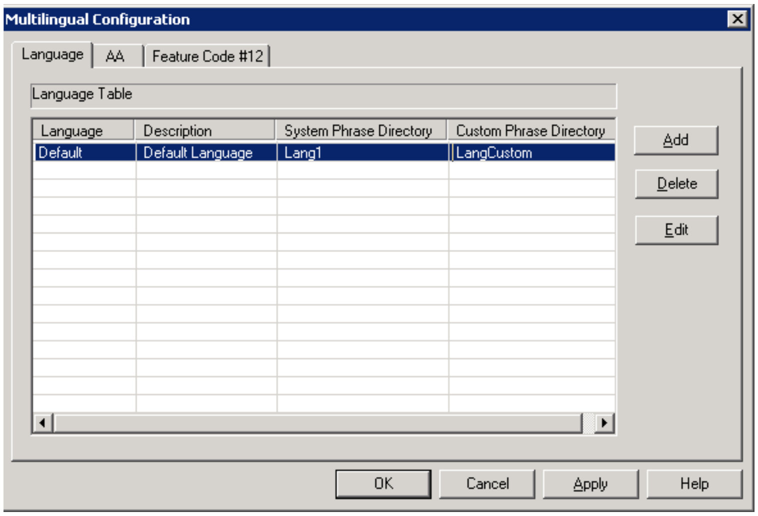
Phrases for language *X* should be saved in a pair of directories: Lang_X and LangCustom_X. Lang_*X* stores the phrases required by the system, and LangCustom_*X* stores your custom phrases.

For example, to add a language for Mexico, you need to create two directories:

- Lang_Mexico
- LangCustom_Mexico

Configuring for a Multilingual System

To configure MaxACD as a multilingual system, select **System** > **Multilingual Configuration**. The Multilingual Configuration screen opens to the **Language** tab. Here you will add references to the language directories you created. These are the directories that contain phrases in other languages.



Language Table

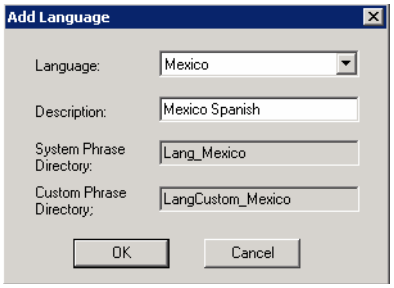
Language	Description	System Phrase Directory	Custom Phrase Directory
Default	Default Language	Lang1	LangCustom

Figure 8-2. Multilingual Configuration, Language tab

When you first run MaxACD, only the default language is listed in the Multilingual Configuration screen, and the description of the default language is displayed as **Default Language**. Each language added to the table will have a formal name, a description, a system phrase directory (LangDir_*X*), and a custom phrase directory (LangCustomDir_*X*), as shown in the previous figure.

To add a language:

1. Click the **Add** button.



Language: Mexico

Description: Mexico Spanish

System Phrase Directory: Lang_Mexico

Custom Phrase Directory: LangCustom_Mexico

Figure 8-3. All Language dialog box

2. Choose a language from the drop-down list. The list shows the language directories you have added to the C:\PostOffice\Phrases directory.
3. Enter a description for the language. This description will appear elsewhere in the graphical user interface, for example in the **Extension Configuration** window and the **AA** tab in this screen.

4. Click **OK**.
5. Repeat these steps for each language you want to add.

The contents of the fields **System phrase directory** and **Custom phrase directory** are fetched from the location where the language phrases are stored. They are not editable.

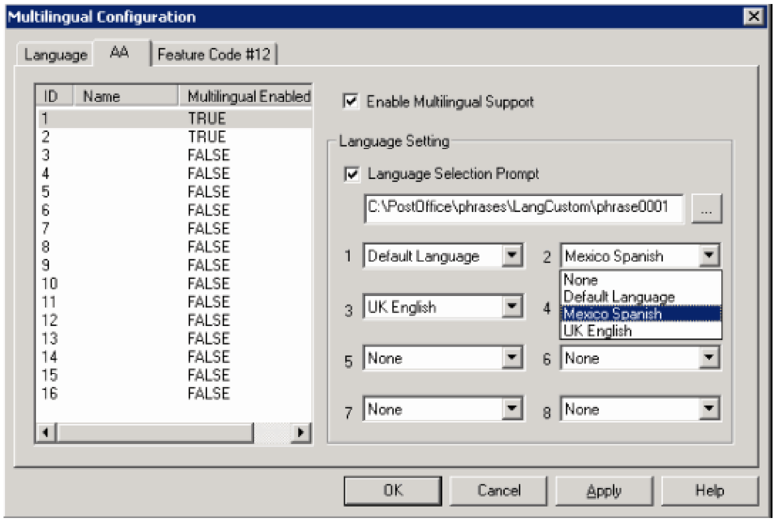
Only the description of the language is editable here. To edit it, click the **Edit** button or double-click the row.

The default language cannot be deleted. After you add languages, any language used by DNIS, an extension, or an AA cannot be deleted.

Enabling Multilingual Support in the Auto Attendant

After you have recorded phrases and added a reference to their directories in the **Multilingual Configuration > Language** tab, as described above, you are ready to enable multilingual support in the auto attendant.

1. Select **System > Multilingual Configuration > AA** tab.



ID	Name	Multilingual Enabled
1		TRUE
2		TRUE
3		FALSE
4		FALSE
5		FALSE
6		FALSE
7		FALSE
8		FALSE
9		FALSE
10		FALSE
11		FALSE
12		FALSE
13		FALSE
14		FALSE
15		FALSE
16		FALSE

☑ Enable Multilingual Support

Language Setting

☑ Language Selection Prompt

C:\PostOffice\phrases\LangCustom\phrase0001

1 Default Language
2 Mexico Spanish (None, Default Language, Mexico Spanish, UK English)
3 UK English
4
5 None
6 None
7 None
8 None

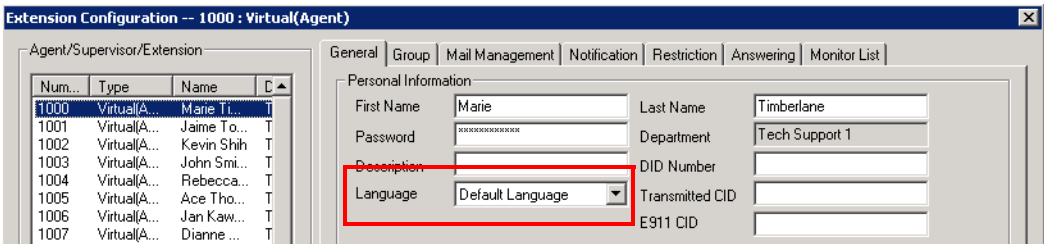
Figure 8-4. Multilingual Configuration dialog box

2. From the list at the left, select the AA you want to configure with multilingual support.
3. Check the **Enable Multilingual Support** box. The **Multilingual Enabled** column changes to **TRUE**.
4. In the **Language Setting** group of fields, check the **Language Selection Prompt** check box.
5. Choose the prompt that lets the caller select a language.
6. Beside each appropriate number, select a language from the drop-down list that corresponds to the phone key the user would press to hear that language. (For example, “For English, press 1; for Spanish, press 2...”)
7. Click **Apply** if you have more work to do in the configuration screen, or click **OK** to accept the changes and close the screen.

Note: This configuration is on top of the regular AA configuration. The system will execute the regular AA action items after a language preference is selected by the caller.

Configuring the Extension

Extension users have a default language configured, and that language is always used for them whenever they hear a prompt on their extension. The default language is assigned in **Extension Configuration** > **General** tab.



Extension Configuration -- 1000 : Virtual(Agent)

Agent/Supervisor/Extension

Num...	Type	Name	D
1000	Virtual(A...	Marie Ti...	T
1001	Virtual(A...	Jaime To...	T
1002	Virtual(A...	Kevin Shih	T
1003	Virtual(A...	John Smi...	T
1004	Virtual(A...	Rebecca...	T
1005	Virtual(A...	Ace Tho...	T
1006	Virtual(A...	Jan Kaw...	T
1007	Virtual(A...	Dianne ...	T

Personal Information

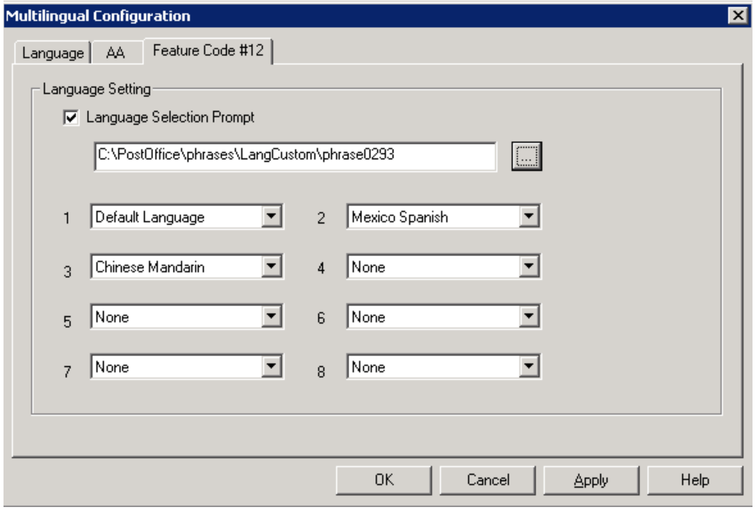
First Name: Marie
Last Name: Timberlane
Password: ************
Department: Tech Support 1
Description:
DID Number:
Language: Default Language
Transmitted CID:
E911 CID:

Figure 8-5. Selecting a language for an extension user

In the **Language** drop-down list, select the desired language, and click **OK**.

Extension User Can Change Language Setting

Extension users can change the extension's language setting by using feature code #12, if feature code #12 is configured on the **System > Multilingual Configuration** > **Feature Code** tab:



Multilingual Configuration

Language Setting

☑ Language Selection Prompt

C:\PostOffice\phrases\LangCustom\phrase0293

1 Default Language
2 Mexico Spanish
3 Chinese Mandarin
4 None
5 None
6 None
7 None
8 None

Figure 8-6. Configuring feature code #12 to let user change a language selection

To configure feature code #12 for language selection:

1. Check the **Language Selection Prompt** check box.
2. Select the prompt the extension user will hear after pressing **#12**. You must know the text of this prompt, so you can match the languages to the correct numbers in the next step.

   For example, the prompt the extension user might hear after pressing #12 might be "To change the preferred language for this extension, press 1 for English, press 2 for Spanish, press 3 for Chinese."
3. Beside each number, select a language from the drop-down list that corresponds to the prompt. The languages listed are those that you have added to MaxACD on the **Language** tab of this window.

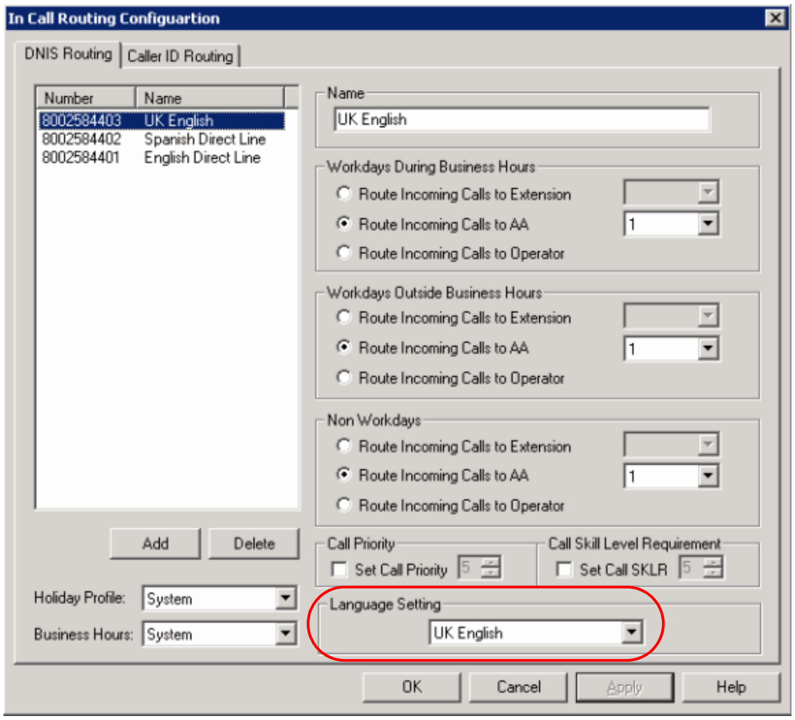
   For example, if you were working from the example prompt in step 2, you would select **English** beside the number 1, **Spanish** beside the number 2, and **Chinese** beside the number 3. The remaining fields would be left as **None**.

Using DNIS to Set the Language

If your company has multiple phone numbers, you can configure MaxACD to direct a caller to prompts in a selected language based on the phone number the caller has dialed.

To direct specified DNIS calls to a selected-language AA or extension:

1. Select **General > In Call Routing Configuration > DNIS Routing** tab.
2. Click **Add**.
3. Select where you want to route callers who have dialed that number.
4. Select the appropriate language from the **Language Setting** drop-down list.
5. Click **Apply**.



In Call Routing Configuartion

DNIS Routing | Caller ID Routing

Number	Name
8002584403	UK English
8002584402	Spanish Direct Line
8002584401	English Direct Line

Name: UK English

Workdays During Business Hours
- ○ Route Incoming Calls to Extension
- ● Route Incoming Calls to AA: 1
- ○ Route Incoming Calls to Operator

Workdays Outside Business Hours
- ○ Route Incoming Calls to Extension
- ● Route Incoming Calls to AA: 1
- ○ Route Incoming Calls to Operator

Non Workdays
- ○ Route Incoming Calls to Extension
- ● Route Incoming Calls to AA: 1
- ○ Route Incoming Calls to Operator

Call Priority: □ Set Call Priority 5

Call Skill Level Requirement: □ Set Call SKLR 5

Language Setting: UK English

Holiday Profile: System

Business Hours: System

Figure 8-7. Configuring the language setting in DNIS

See “DNIS Routing” on page 111 for rules and restrictions on routing using DNIS.

Which Language Will Be Used?

MaxACD follows these rules to determine which language to use:

1. The extension user hears the prompts in the language configured or selected via the **#12** feature code.
2. If the external caller selects a language in the auto attendant, MaxACD uses the selected language. If a language selection is invalid or times out (7 seconds) three times in a row, the default language is selected.
3. When the user logs in to the voice mail of an extension, the extension's language is used.
4. If DNIS is configured for language setting, the external caller hears the prompts in the language specified by the number he dialed.
5. In any other case, the system default language is used.

CHAPTER

9

Call Recording Configuration

To use the centralized call recording function, make sure the following requirements are met:

- You need a recording seat license for each extension that will be recording.
- It is recommended that you have a separate storage server to store recorded files.
- Recorded files (64Kbps PCM format) can be managed by the VRManager (licensed) application or can simply be saved and played with VRPlayer (free).
- If your system has a multi-chassis configuration and the gateway needs to transmit recorded files to a storage server, you need to set up an FTP server to facilitate the file transfer. You do *not* need to set up an FTP server for a single chassis (all-in-one) installation.
- Because recording files requires a large amount of disk storage space, NAS (Network Attached Storage) system is recommended, unless VRManager is used.

Description of the Recorded File Name

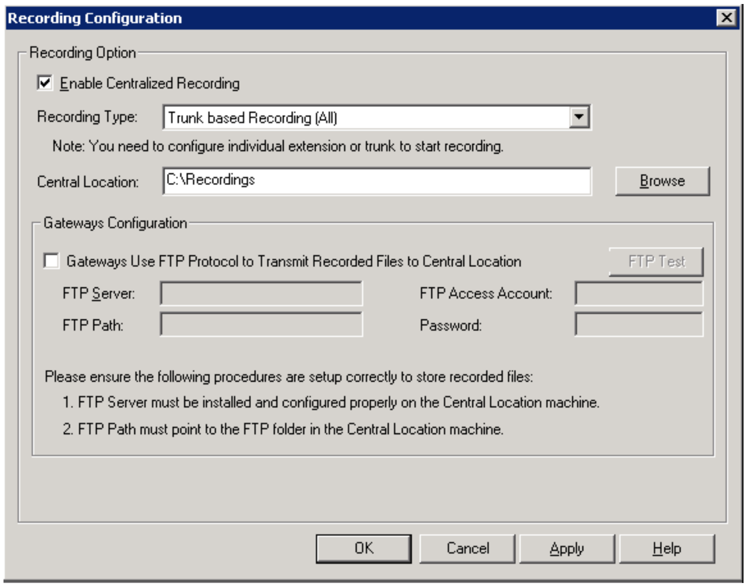
The recorded file name contains the following information:

- R!**mmddyyyy_hhmmss!callerID!calleeID!workgroupID!DNIS!sessionID**!R
- **mmddyyyy_hhmmss** is the time stamp when the recording starts
- **callerID** is the caller ID or extension number. It could also be:
  - **bgn** for barge-in call
  - **sm** for a silent monitor call
  - **trk(bbcc)** for an inbound trunk call without caller ID. *bb* is the board logical ID and *cc* is the channel ID
- **calleeID** is the target number or **trk**(bbcc)
- **workgroupID** is the workgroup number for a workgroup call, or **ext** for extension call
- **DNIS** is the DNIS number or NA for no DNIS number
- **sessionID** is the CDR session ID

Configuring Call Recording

To configure system-wide call recording, including centralized recording for multiple gateways, do one of the following:

- Click the **Recording** button on the toolbar.
- Select **System > Call Recording Configuration**.



Recording Configuration

Recording Option

☑ Enable Centralized Recording

Recording Type: Trunk based Recording (All)

Note: You need to configure individual extension or trunk to start recording.

Central Location: C:\Recordings

Gateways Configuration

☐ Gateways Use FTP Protocol to Transmit Recorded Files to Central Location

FTP Server:

FTP Access Account:

FTP Path:

Password:

Please ensure the following procedures are setup correctly to store recorded files:

1. FTP Server must be installed and configured properly on the Central Location machine.
2. FTP Path must point to the FTP folder in the Central Location machine.

Figure 9-1. Recording Configuration window

Note: Call recording options for specific extensions/workgroups can be set up on the **General** tab of **Extension Configuration** and **Workgroup Configuration**, respectively.

To Enable and Configure Centralized Recording

1. Check the **Enable Centralized Recording** check box.
2. Select a **Recording Type** from the drop-down list.
3. In the **Central Location** field, browse for the directory you want to set as the destination folder and path for saving the call recordings.

   Important: If you are using FTP protocol, the FTP server must be installed and configured properly on the same machine as the **Central Location** directory.

   An FTP folder must be created for the **Central Location**, so that it can be fully accessible through FTP.

   The **FTP Path** must be pointed to the **Central Location**.
4. If you are using multiple gateways, and you are *not* using network attached storage, check **Gateways Use FTP Protocol to Transmit Recorded Files to Central Location**.

   a. **FTP Server**—Enter the IP address of the FTP server.

   b. **FTP Access Account**—An FTP server account name that gateways can log in to.

   c. **FTP Path**—Enter the directory that the files will be transmitted to on the FTP server.

   d. **Password**—FTP account password.

5. Click the **FTP Test** button to verify that login to the FTP server is successful.
6. When you are finished configuring, click **OK**.

Using a Remote Shared Directory

It is strongly recommended that you use VRManager to manage centralized recording and that you save recordings to a local drive or network attached storage on the gateway that is running MaxACD. If you save recordings to a network drive, and the network becomes unstable, you could lose any files of conversations being recorded at that time.

CHAPTER

10

Application Extension Configuration

The application extension is an extension pilot number that allows an SDK-based add-on application to log into the system and establish a communication channel to control trunk channels and interact with the system core switching and voice processing service.

Typical applications that use an application extension are:

- IVR
- Outbound dialer
- Inbound call routing logic for a special business application

To connect an SDK-based add-on application, you need:

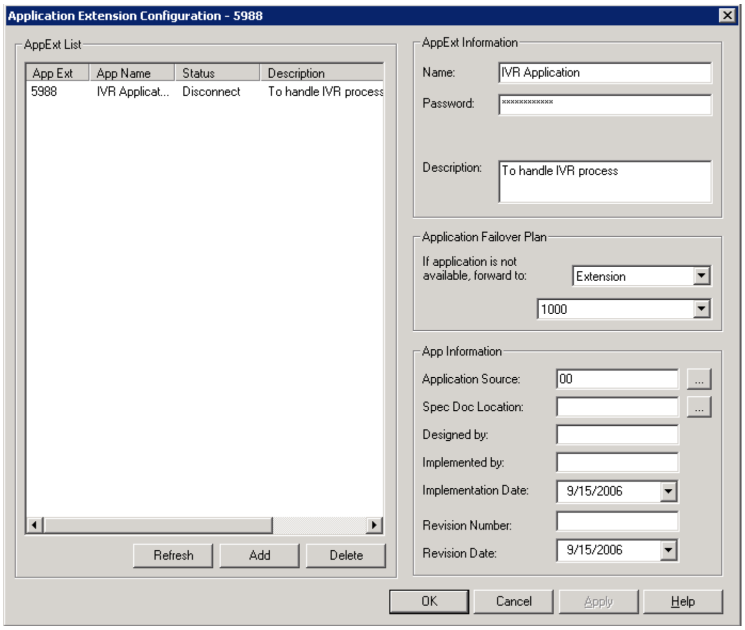
- An APC license (concurrent session)
- A separate application extension to log in to for each application

For more information about SDK, please send e-mail to sdksupport@altigen.com.

Application Extension Setup

Note: Before you begin, make sure a **Trunk Control APC SDK Session** license is registered and activated for your system. You can find this information in **License** > **License Information**.

To access the **Application Extension Configuration** window, select **System > Application Ext Configuration**.


Application Extension Configuration - 5988

AppExt List

App Ext	App Name	Status	Description
5988	IVR Applicat...	Disconnect	To handle IVR process

AppExt Information

Name: IVR Application

Password: ************

Description: To handle IVR process

Application Failover Plan

If application is not available, forward to: Extension

1000

App Information

Application Source: 00

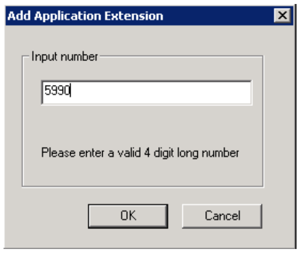
Implementation Date: 9/15/2006

Revision Date: 9/15/2006

Figure 10-1. Application Extension Configuration window

To set up an application extension:

1. In the Application Extension Configuration window, click the **Add** button and enter an extension number in the **Add Application Extension** dialog box. and click **OK**.


Add Application Extension

Input number: 5990

Please enter a valid 4 digit long number

Figure 10-2. Add Application Extension dialog box

2. The application extension appears in the **AppExt List**.
3. Type a password in the **Password** field.
4. Type a description of the application in the **Description** field, if desired.
5. Click **OK**.

Application Failover Plan

The **Application Failover Plan** ensures that a call made to the extension will be automatically transferred if the application is not available. Use the **If application is not available, forward to** drop-down list to select the forwarding destination. The options are:

- **AA**—select the auto attendant number to use in the drop-down list under the option. AA settings are configured in **System > AA Configuration**.
- **Extension**—select an extension from the drop-down list.
- **Operator**—select an operator from the drop-down list.

Important: If the failover setting for the application extension is set to an extension, and the extension is RNA or busy, the call will follow the extension's RNA or busy call handling.

Application Information

Additional information can be described in the **App Information** fields. If desired, enter the appropriate information in the fields for **Application Source**, **Spec Doc Location**, **Designed by**, **Implemented by**, **Implementation Date**, **Revision Number** and **Revision Date**.

Readying the Application

If a third-party application is connecting to this extension, make sure the application is properly set to log into the application extension. If the third-party application is logged in, the status shown in Figure 10-1, "Application Extension Configuration window" changes to "connected."

CHAPTER

11

Component Configuration

This section shows how to configure MaxACD for Lync components:

- Virtual component SIPSP; see “Configuring Virtual Component SIPSP” on page 91
- HMCP components; see “Configuring Virtual Component HMCP” on page 92

Configuring Virtual Component SIPSP

A VoIP connection typically consists of two parts:

- **Signal Channel**—responsible for setting up and tearing down a call using protocol. For example, SIP protocol is used in MaxACD to build a signal channel between the server and the IP phone.
- **Media Path**—responsible for encoding, transmitting, and decoding voice for both parties. For example, when an IP phone user makes a call to an outside number, the voice will be encoded at the IP phone, transmitted to the system via the IP network, decoded by the VoIP codec, and passed to a trunk port so that the external party will hear the voice.

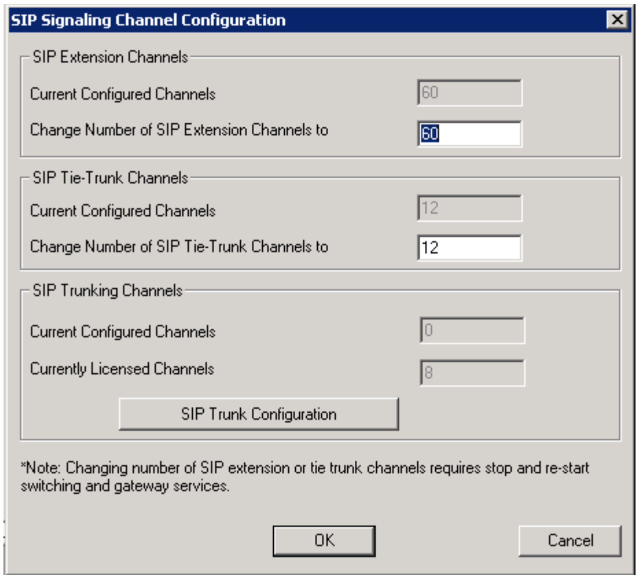
The purpose of virtual component SIPSP is to build signal channels for different connection types, IP extensions, SIP Tie Trunks, and SIP Trunking from ITSP. Each channel will have its channel ID. When an IP phone registers to the system, a channel ID will be assigned to the IP extension. However, these channels are only responsible for processing protocol and call control signals. They require a media path from a VoIP component or from the IP phone to establish a voice steam so that both sides can hear.

Notes:

- Make sure you have enough IP resources from HMCP media server.
- The more signal channels, the more system memory and CPU power required. Proper planning is essential.
- Changing the number of signal channels requires that you stop and restart the switching and gateway services.
- SIP Trunking Channel requires a license to activate.

To open the configuration dialog box,

1. Double-click a SIPSP component in **Components** view.
2. Click the **Component Configuration** button



SIP Signaling Channel Configuration

SIP Extension Channels

Current Configured Channels: 60

Change Number of SIP Extension Channels to: 60

SIP Tie-Trunk Channels

Current Configured Channels: 12

Change Number of SIP Tie-Trunk Channels to: 12

SIP Trunking Channels

Current Configured Channels: 0

Currently Licensed Channels: 8

*Note: Changing number of SIP extension or tie trunk channels requires stop and re-start switching and gateway services.

If you change the number of SIP extensions or tie trunk channels, you must stop and restart the switching and gateway services.

Figure 11-1. SIP Signaling Channel Configuration dialog box

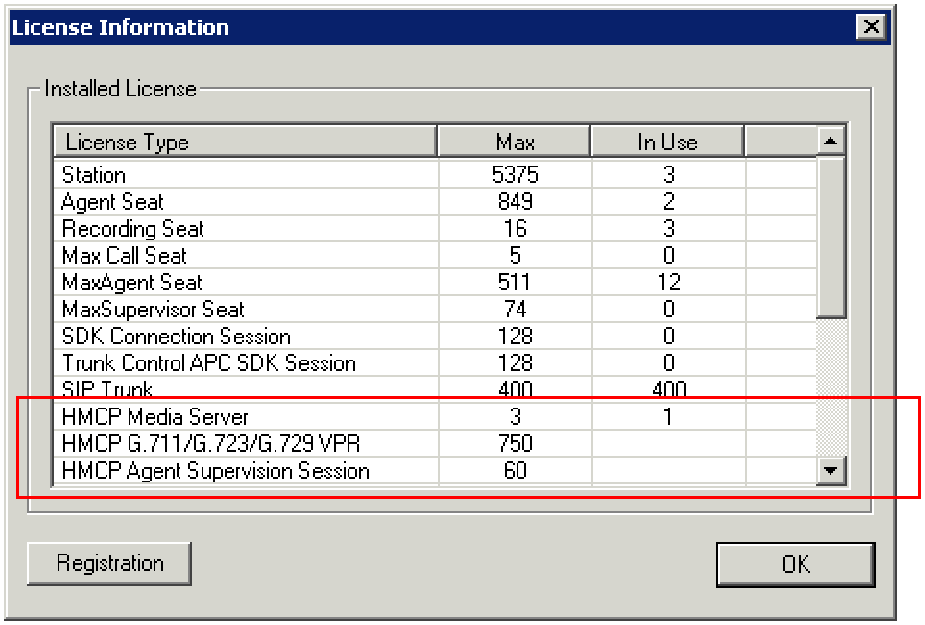
The number of configured channels and licensed channels are displayed.

MaxACD is set by default to support 60 SIP extension channels. You can change the number of SIP extension channels and tie-trunk channels. The maximum number possible depends of the system CPU performance, call volume, and usage. If a high performance machine is used as the MaxACD server, the number of channels can be more than 1000. If you change the numbers in this dialog box, you must shut down and restart the switching and gateway services for this change to take effect. When the services restart, the new configuration appears in the **Currently Configured Channels** fields.

The **SIP Trunking Configuration** button in this dialog box opens the SIP Trunking Configuration dialog box. (See “SIP Trunk Properties” on page 102.)

Configuring Virtual Component HMCP

Note: An AltiGen HMCP Media Server license is required to activate an HMCP media server.



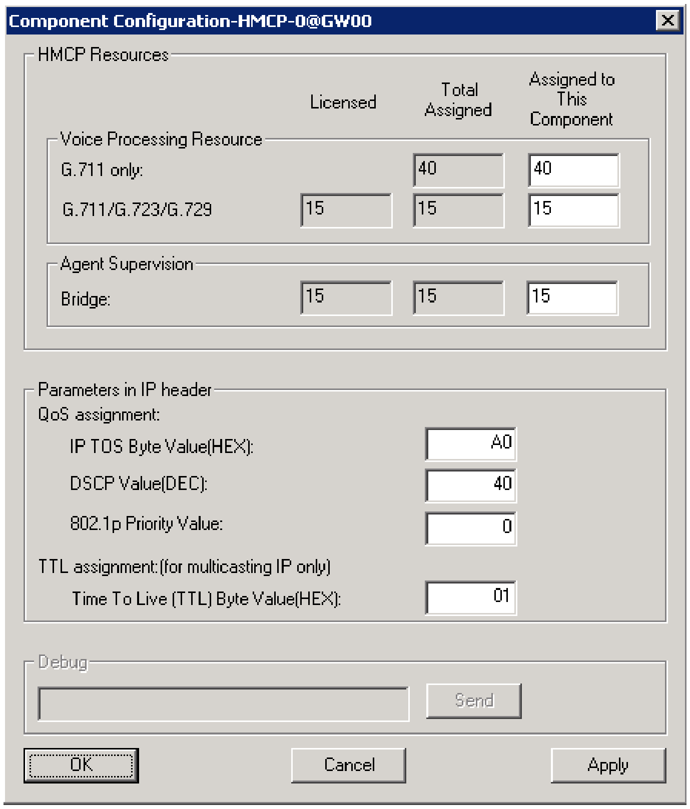
License Type	Max	In Use
Station	5375	3
Agent Seat	849	2
Recording Seat	16	3
Max Call Seat	5	0
MaxAgent Seat	511	12
MaxSupervisor Seat	74	0
SDK Connection Session	128	0
Trunk Control APC SDK Session	128	0
SIP Trunk	400	400
HMCP Media Server	3	1
HMCP G.711/G.723/G.729 VPR	750	
HMCP Agent Supervision Session	60	

Figure 11-2.   License Information dialog box

HMCP (Host Media Control Processing) is a virtual component that uses an Intel CPU to provide the following functions:

1. Process VoIP Media Stream
   - Encode, decode, and transcode voice stream
   - Detect and generate tone for IP devices
   - Play music when device is on hold
   - Process IP paging
2. Play and Record Voice Files
   - Announce system and queue phrases
   - Process auto attendant
   - Process voice mail
   - Call recording
3. Provide Conferencing Resources
   - Barge-in/silent monitor/coaching

You can configure HMCP resources, by double-clicking an HMCP component in Components view and then clicking the **Component Configuration** button to open this dialog box:



Component Configuration-HMCP-0@GW00

HMCP Resources

	Licensed	Total Assigned	Assigned to This Component
Voice Processing Resource			
G.711 only:		40	40
G.711/G.723/G.729	15	15	15
Agent Supervision			
Bridge:	15	15	15

Parameters in IP header

QoS assignment:

IP TOS Byte Value(HEX): A0

DSCP Value(DEC): 40

802.1p Priority Value: 0

TTL assignment:(for multicasting IP only)

Time To Live (TTL) Byte Value(HEX): 01

Figure 11-3.   Component Configuration dialog box

If you increase or decrease the number of HMCP resources, you must reboot the system (both the primary and secondary servers) so that the changes can take effect.

If your HMCP server is outside of the MaxACD system, then you must restart the HMCP server first, before restarting the primary and secondary servers.

You may change the assigned number by entering a different number (up to the number your system is licensed for and not to exceed the maximum limit for each HMCP component) in the **Assigned to this component** fields and clicking **Apply**.

HMCP Resources—Shows the total number licensed (if applicable), total currently assigned, and the number assigned to this HMCP component for the following resource types:

1. Voice Processing Resources (VPR)
2. Agent Supervision Bridges

The maximum number of resources that can be assigned to each HMCP virtual component is as follows:

- G.711 VPR — 1,000
- G.711/G.723/G.729 VPR — 200
- Agent Supervision Bridges — 20

Notes:

- 1,000 G.711 voice processing resources will be licensed to the system when one AltiGen HMCP Media Server license is registered.
- The more VPR assigned, the slower the system will be when it starts up. To calculate the optimized number of VPR you need, use the following formula:

  Total G.711 VPR = Total number of extensions X 2

Total G.711/723/729 VPR = Total of SIP Trunks + Total Tie Trunk Channels that will use compressed codec

- Adding HMCP licenses or changing assigned numbers does not require restarting the MaxACD switching service.
- In the event that you need to decrease the assigned numbers of HMCP resources (reassigned to the second HMCP server, for example), the system must be rebooted for the configuration to take effect.

Parameters in IP Header—QoS and TTL assignments.

QoS assignment—IP TOS/DiffServ Byte Value. The default TOS/DiffServ byte hex value "A0" (10100000) signals the network switch and router that RTP packets are "Critical". To set the value for Diffserv Code Expedited Forwarding (DSCP EF), you can enter hex value "B8" (10111000).

TTL assignment—for IP paging multicasting only. The purpose of the TTL (Time To Live) is to regulate how many hosts the IP paging packets can pass through. The TTL value is reduced by one on every hop. You may need to adjust this value if there are remote IP phones at different locations that register to MaxACD through WAN and require the IP paging feature. The value will be the number of routers from MaxACD to remote IP phone plus one.

Note: In order to use the QoS parameters in IP headers, you must first install the NetFilter driver. To do this, run *setup.exe* in the NetFilter Driver folder on your MaxACD install CD.

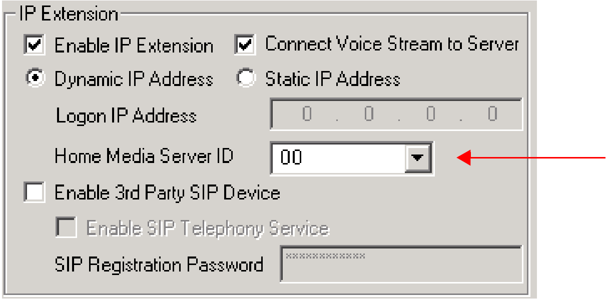
Assign HMCP Resources to Extensions

After you configure the HMCP component, you need to configure extensions to use the HMCP voice processing and recording resources.

In **Extension Configuration > General > IP Extension** panel, change the **Home Media Server ID** to the HMCP Media Server ID if necessary. Please refer to the following scenarios.

Scenario 1 - HMCP Media Server inside MaxACD Server

For fewer than 200 agents, you may consolidate the MaxACD and HMCP into one server. The IP extension Home Media Server ID should be assigned to "00" by default. You do not need to change this number since both MaxACD and HMCP media server are in the ID "00".



IP Extension

☑ Enable IP Extension ☑ Connect Voice Stream to Server

● Dynamic IP Address ○ Static IP Address

Logon IP Address 0 . 0 . 0 . 0

Home Media Server ID 00

☐ Enable 3rd Party SIP Device

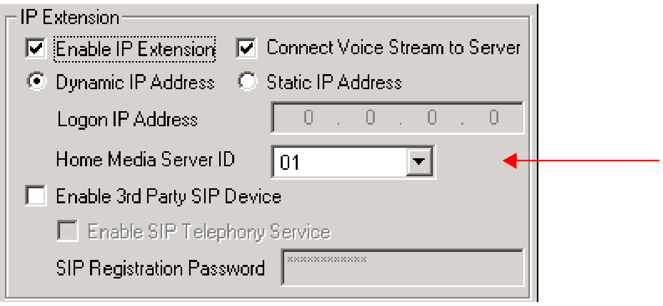
☐ Enable SIP Telephony Service

SIP Registration Password ************

Figure 11-4. HMCP Media Server inside MaxACD Server

Scenario 2: Single Standalone HMCP Media Server

For 200 to 1,000 agents without an extensive amount of recording resources, and fewer than 200 concurrent recording sessions, you may deploy a stand-alone HMCP media server. The Home Media Server ID should be changed to "01" for all extensions, assuming HMCP media server is using ID 01.



IP Extension

☑ Enable IP Extension ☑ Connect Voice Stream to Server

● Dynamic IP Address ○ Static IP Address

Logon IP Address 0 . 0 . 0 . 0

Home Media Server ID 01

□ Enable 3rd Party SIP Device

□ Enable SIP Telephony Service

SIP Registration Password

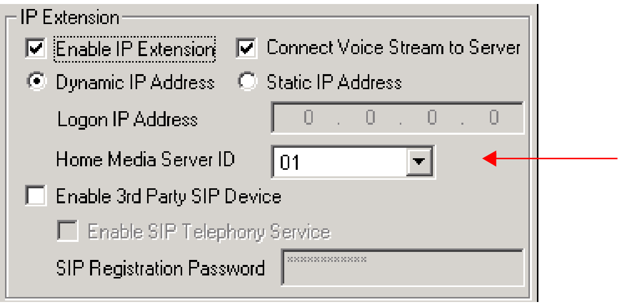
Figure 11-5. Single Standalone HMCP Media Server

Scenario 3: Multiple HMCP Media Servers

For large call center agent installations, you may deploy multiple HMCP media servers to achieve load balancing and failover protection.

To achieve load balancing, you need to divide and assign extensions to different Home Media Server IDs. The following guidelines may help you make decisions when assigning extensions to different Home Media Server IDs.

- Equally divide the extensions that require centralized recording and assign them to different HMCP media servers.
- Assign extensions in a department to the same media server.



IP Extension

☑ Enable IP Extension ☑ Connect Voice Stream to Server

● Dynamic IP Address ○ Static IP Address

Logon IP Address 0 . 0 . 0 . 0

Home Media Server ID 01

□ Enable 3rd Party SIP Device

□ Enable SIP Telephony Service

SIP Registration Password

Figure 11-6. Multiple HMCP Media Servers

If you have two or more HMCP media servers, the system will provide failover in the event that one media server is off-line. When the home media server for an IP extension is not available, the media manager in the system will search available resources from other media servers when that extension requests media service. This will happen atomatically (no configuration required) and dynamically (the resource may come from a different media server each time that extension requests a media resource).

CHAPTER

12

Trunk Configuration

Trunk attributes and parameters are set using the **Trunk Configuration** window. The attributes and options available depend on the type of component and trunk. This chapter discusses general configuration options applicable to all trunks, followed by specific configuration options for the following trunk types:

- SIP tie trunk, "SIP Tie Trunk Properties" on page 101
- SIP trunk for ITSP, "SIP Trunk Properties" on page 102

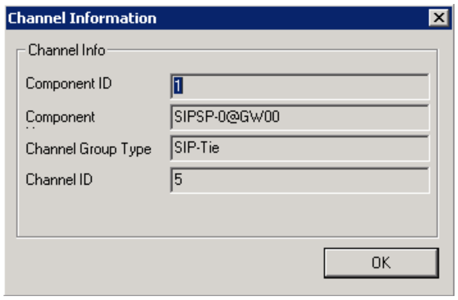
This chapter also discusses incoming call routing ("Incoming Call Routing" on page 106) and outgoing call blocking ("Outgoing Call Blocking" on page 107), both configurable on tabs in the **Trunk Configuration** window.

Trunks Out of Service

If none of the trunks are available when an outside call is placed, the caller will hear the system prompt: "All outside lines are busy. Please try again later."

Channel Identification

To find out channel information, right-click a trunk in the Trunk View window (shown in Figure 12-2, below), and select **Channel Physical Location**. The Channel Information box appears, displaying component ID, component name, channel group type, and channel ID:



Component ID 1

Component SIPSP-0@GW00

Channel Group Type SIP-Tie

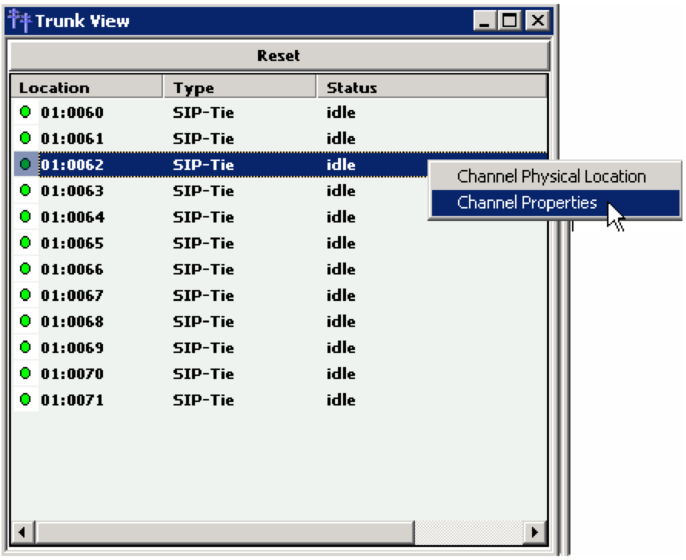
Channel ID 5

Figure 12-1. Channel Information box

Opening the Trunk Configuration Window

To open the general **Trunk Configuration** window, do one of the following:

- Click the **Trunk Configuration** button in the toolbar.
- Select **General > Trunk Configuration**.
- Double-click a trunk in the **Trunk View** window.

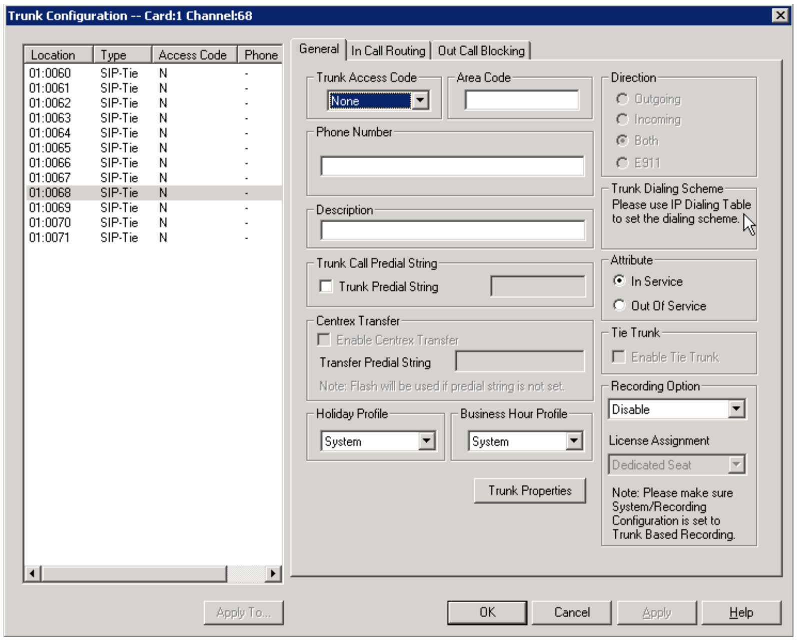


Location	Type	Status
01:0060	SIP-Tie	idle
01:0061	SIP-Tie	idle
01:0062	SIP-Tie	idle
01:0063	SIP-Tie	idle
01:0064	SIP-Tie	idle
01:0065	SIP-Tie	idle
01:0066	SIP-Tie	idle
01:0067	SIP-Tie	idle
01:0068	SIP-Tie	idle
01:0069	SIP-Tie	idle
01:0070	SIP-Tie	idle
01:0071	SIP-Tie	idle

Selecting Channel Properties from the right-click menu in Trunk View bypasses the general Trunk Configuration window to open a trunk properties window specific to the selected trunk.

Figure 12-2. Trunk View window

The Trunk Configuration window opens:



Trunk Configuration -- Card:1 Channel:68

Location	Type	Access Code	Phone
01:0060	SIP-Tie	N	-
01:0061	SIP-Tie	N	-
01:0062	SIP-Tie	N	-
01:0063	SIP-Tie	N	-
01:0064	SIP-Tie	N	-
01:0065	SIP-Tie	N	-
01:0066	SIP-Tie	N	-
01:0067	SIP-Tie	N	-
01:0068	SIP-Tie	N	-
01:0069	SIP-Tie	N	-
01:0070	SIP-Tie	N	-
01:0071	SIP-Tie	N	-

Trunk Access Code: None

Area Code:

Phone Number:

Description:

Direction: ○ Outgoing ○ Incoming ● Both ○ E911

Trunk Dialing Scheme: Please use IP Dialing Table to set the dialing scheme.

Trunk Call Predial String: □ Trunk Predial String

Attribute: ● In Service ○ Out Of Service

Centrex Transfer: □ Enable Centrex Transfer

Transfer Predial String

Note: Flash will be used if predial string is not set.

Tie Trunk: □ Enable Tie Trunk

Recording Option: Disable

License Assignment: Dedicated Seat

Holiday Profile: System

Business Hour Profile: System

Note: Please make sure System/Recording Configuration is set to Trunk Based Recording.

Figure 12-3. Trunk Configuration, General tab

Selecting Trunks to Set Attributes

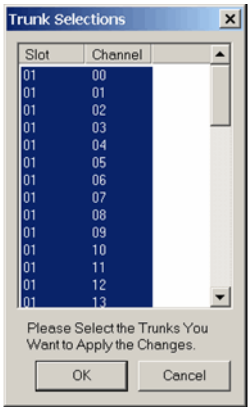
The title bar of the Trunk Configuration window displays the card and the channel of the selected trunk.

The list on the left shows all the configured trunks. The **Location** format is the same as in the Trunk View window, that is, *Logical Component ID : Channel number*. The logical component ID is assigned by the system. This ID may change when a component is added into or removed from the system.

When you select a trunk in this list, the options and parameters for the trunk appear in the settings in the right side of the window.

Configuring One or Multiple Trunks

To customize trunk characteristics, you work on one trunk at a time. To apply the same configuration to multiple trunks, use the **Apply To** button. This pops up a list of all trunks, with all of the trunks selected by default. Select the trunks you want to apply changes to, then click **OK**. (Use **Ctrl**+click and **Shift**+click to select several trunks.) This applies changes to multiple trunks for *only the attribute or option that you changed***.**



Slot	Channel
01	00
01	01
01	02
01	03
01	04
01	05
01	06
01	07
01	08
01	09
01	10
01	11
01	12
01	13

Please Select the Trunks You Want to Apply the Changes.

Figure 12-4. Selecting trunks to configure

Setting General Trunk Attributes

Select a channel to view its current attributes. You can then set or change the following attributes. If an option is grayed out, it is not available for that type of trunk:

- **Access Code**—Assign a trunk access code to the selected trunk. If you need to use a trunk access code other than 9, you must first set this up on the **Number Plan** tab of **System Configuration** (see “Setting a System Number Plan” on page 35).

  Note: There are two types of access code: Trunk Access Code (TAC) and Route Access Code (RAC). TAC is a quick and easy way to select which trunk(s) you would like to dial out from, especially when you want to reserve trunks for a special dialing purpose. For example, you can set up TAC "7" and assign that to trunk(s). These trunks will be reserved exclusively for users who know the TAC "7".

  Although TAC is easy to use, it does have limitations especially when you are located in an area with a complicated dialing pattern or you need to set up VoIP hop-off dialing.

  RAC uses the Out Call Routing table, which has the flexibility to group trunks into a route, assign routes to a specific dialing pattern, and add/delete digits from the dialing pattern. It can solve most of the complicated dialing problems. If your system is using RAC, you can set this TAC field to "None".

- **Area Code**—The local area code for each trunk. Enter a three-digit area code. If left blank, the trunk assumes the home area code defined in the **General** tab of the System Configuration window. *This configuration is for each trunk in the system and will negatively affect features such as Zoomerang if the area code is not configured prope*rly.

- **Direction**—The trunk direction can be **Outgoing** only, **Incoming** only, or **Both** Outgoing and Incoming. The **Both** option is the system default.

- **Phone Number**—Enter the number without area code in this field.

  Trunk transmitting caller ID rules:

  1. If extension has **Transmitted CID** configured, this number will be transmitted first. If not configured, go to next.
  2. If extension has **DID Number** configured, the 10-digit DID number will be transmitted. If not configured, go to next.

3. If PRI trunk channel has area code and caller ID configured, this number will be transmitted. If not configured, go to next.
4. PRI will transmit the system home area code and main number defined in System Configuration, **General** tab.

- **Description**—Descriptive information such as the company name for the assigned Phone Number.
- **Trunk Dialing Scheme**—For IP tie trunks, use the IP Dialing Table in Enterprise Manager to set the dialing scheme (Enterprise Manager is available by selecting **VoIP > Enterprise Network Management**, or from the Windows **Start** menu).
- **Trunk Call Predial String**—To have the system automatically insert the configured digits whenever the selected trunk is used for outgoing calls.
- **Attribute—In Service** makes the trunk available for use. **Out of Service** prevents the trunk from being used (for example, while performing maintenance).
- **Holiday Profile**—A holiday profile can be assigned to a trunk. The drop-down list selection is based on settings configured in the **Holiday** tab of System Configuration (see "Routing Calls on Holidays" on page 41).
- **Business Hour Profile**—A business hour profile can be assigned to a trunk. The drop-down list selection is based on settings configured in the **Business Hours** tab of System Configuration.
- **Recording Option**—Recording for incoming and outgoing calls is supported. Use the drop-down list to select **Disable** or **Enable**. If you select **Enable**, make sure that in **System > Recording Configuration** one of the trunk-based recording options is selected.

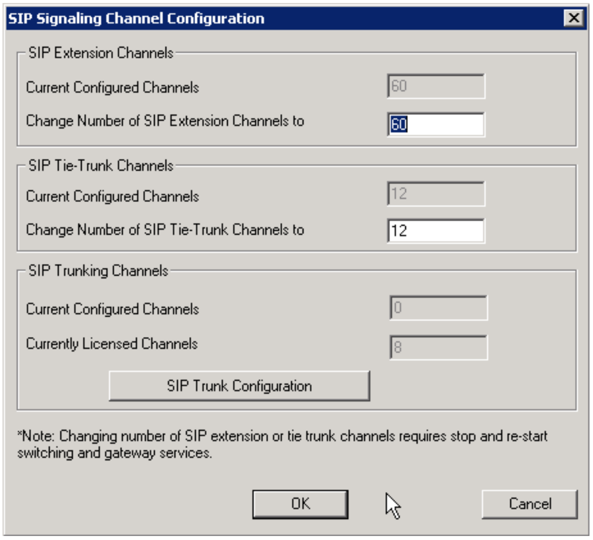
  Note: When you use trunk-based recording, inbound or outbound calls are recorded as long as the trunk is in use. For example, an inbound call that is answered by an AA, routed to an operator, and transferred to an extension will begin recording when the AA answers the call and end recording when the trunk is released.

  With extension recording, recording starts only when the extension user answers the call.
- **Trunk Properties**—Opens a dialog box that allows you to configure properties for each trunk. The options vary depending on the type of trunk; this is discussed in subsequent sections.

SIP Tie Trunk Properties

To open a configuration dialog box for a SIP-tie trunk channel, do one of the following:

- If you're in the **Trunk Configuration** window, select a SIP-Tie channel from the trunk channel list, then click the **Trunk Properties** button, or just double-click the channel in the list.
- If you're in the **Trunk View** window, right-click the channel and select **Channel Properties**.



SIP Signaling Channel Configuration

SIP Extension Channels

Current Configured Channels: 60

Change Number of SIP Extension Channels to: 60

SIP Tie-Trunk Channels

Current Configured Channels: 12

Change Number of SIP Tie-Trunk Channels to: 12

SIP Trunking Channels

Current Configured Channels: 0

Currently Licensed Channels: 8

*Note: Changing number of SIP extension or tie trunk channels requires stop and re-start switching and gateway services.

Figure 12-5. Configuration dialog box for a SIP Signaling channel

See "To open the configuration dialog box," on page 91 for component configuration information.

Note: This is signal only trunks. Make sure you have enough IP resource components to cover your needs.

SIP Trunk Properties

IP dial tone service is delivered through your IP data network, and the service provider can be anywhere in the world, as long as the VoIP data packets can be routed properly.

If you have SIP-based IP dial tone service from an Internet Telephony Service Provider (ITSP), you need to configure SIP trunk channels to connect to the service. Before you start, note the following:

- A MaxACD SIP Trunking channel is licensed. You need to buy and register a license to be able to configure this option.
- AltiGen does not guarantee the voice quality of the SIP dial tone coming from your service provider. You need to work with your data service and SIP trunking service provider to make sure adequate QoS is provisioned for your WAN service.
- AltiGen does not guarantee SIP trunk implementation will work with all SIP dial tone service providers. AltiGen dealers are notified of AltiGen-tested and certified SIP-Trunk service providers. Configuration guidelines for each AltiGen-certified SIP-Trunk service provider can be found in the AltiGen authorized dealer Knowledge Base, available from the AltiGen Dealer Web Site. SIP dial tone service providers need to support the following:
  - G.711, G.723.1, G.729 codec
  - RFC 2833 for DTMF tone delivery
  - SIP MD5 authentication with SIP registration
  - If MaxACD is behind NAT, verify that your SIP SP can support this configuration.

When subscribing to a SIP dial tone service, typically your service provider will provide you with the information required in the configuration dialog box shown in Figure 12-6, “SIP Trunk Configuration dialog box and Edit box". Enter these service parameters to each SIP trunk channel configuration individually.

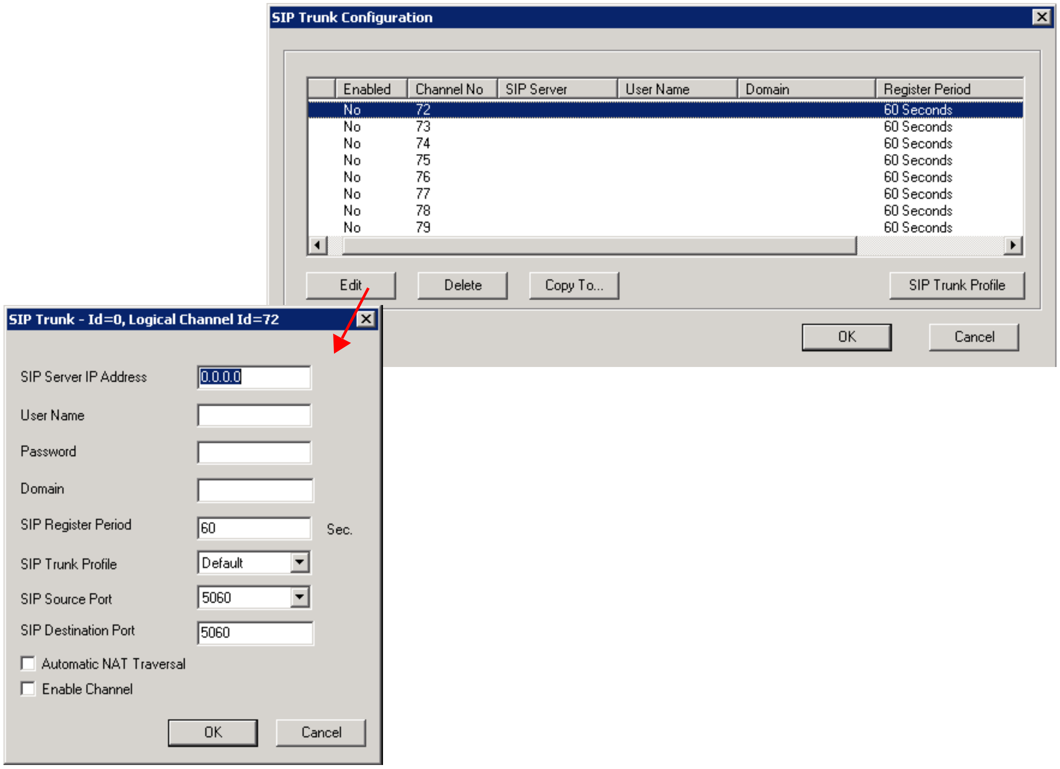
Note: This is signal only trunks. Make sure you have enough IP resource components to cover your needs.

Important: You must add the SIP Trunk service provider’s IP address to the IP Device Range in Enterprise Manager and select the proper codec profile for this service. See “Assigning Codec Profiles to IP Addresses” on page 194. Failure to do this step may cause no voice path, even if the SIP Trunk channel shows the call is connected.

Configuring a SIP Trunk

To open a trunk configuration dialog box for a SIP trunk, do one of the following:

- In the **Trunk Configuration** window, select a SIP trunk type, click the **Trunk Properties** button, then click the **SIP Trunk Configuration** button.
- In the **Component View** window, double-click a SIPSP board type, click the **Component Configuration** button, then click the **SIP Trunk Configuration** button.



Enabled	Channel No	SIP Server	User Name	Domain	Register Period
No	72				60 Seconds
No	73				60 Seconds
No	74				60 Seconds
No	75				60 Seconds
No	76				60 Seconds
No	77				60 Seconds
No	78				60 Seconds
No	79				60 Seconds

SIP Server IP Address: 0.0.0.0

User Name:

Password:

Domain:

SIP Register Period: 60 Sec.

SIP Trunk Profile: Default

SIP Source Port: 5060

SIP Destination Port: 5060

□ Automatic NAT Traversal

□ Enable Channel

Figure 12-6. SIP Trunk Configuration dialog box and Edit box

To edit a line, click the **Edit** button, fill in the blanks, and click **OK**.

- **SIP Server IP Address**—The SIP Trunk service provider’s server IP address

- **User Name**—Assigned by the SIP Trunk service provider
- **Password**—Assigned by the SIP Trunk service provider
- **Domain**—The Domain Name of the SIP Trunk service provider, if required
- **SIP Register Period**—How frequently the MaxACD system needs to send SIP registration packets to the service provider. This can detect if the service provider is up or not. Some service providers do not accept SIP Register messages. In these cases, you can disable sending SIP Register messages from MaxACD by setting the **SIP Register Period** to **0**.
- **SIP Trunk Profile**—Select the appropriate SIP trunk profile. (See "Creating a SIP Trunk Profile" on page 104.)
- **SIP Source Port**—For SIP UDP, select the source port from 5060 or 10060. For TCP or TLS, you cannot change ports. Using a port other than 5060 will prevent SIP-ALG firewall/router from changing the SIP packets.
- **SIP Destination Port**—A SIP Trunk can have different source port and destination port.
- **Automatic NAT Traversal**—Leave this box unchecked.
- **Enable Channel**—After all above parameters are entered correctly, check this box to activate the channel. The MaxACD system will send authentication to the service provider to verify the setting.

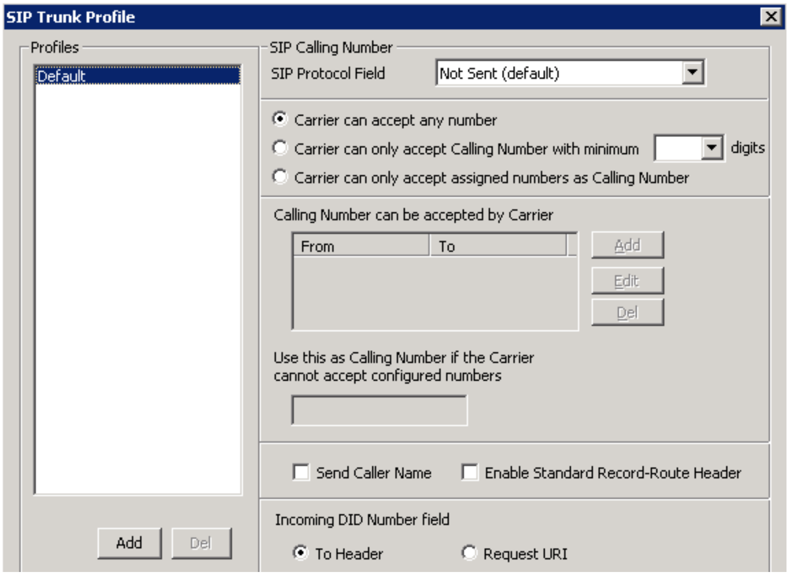
To copy the information in one row to other rows, select the row and click **Copy To**. Then select the rows you want to copy the information to, using **CTRL**+click and **Shift**+click to select several rows. Click **OK**.

To delete a row, select it and click **Delete**.

Creating a SIP Trunk Profile

Different SIP service providers may support different ways of sending a caller ID. To provide callees with a more accurate caller ID, you can create a SIP Trunk Profile for a particular service provider, when necessary. Otherwise, a default profile is used. Once you have created a profile, you can select it in the SIP Trunk Configuration Edit box (see Figure 12-6, "SIP Trunk Configuration dialog box and Edit box").

To create a SIP Trunk Profile, in the SIP Trunk Configuration dialog box shown in Figure 12-6, "SIP Trunk Configuration dialog box and Edit box", click the **SIP Trunk Profile** button on the right.



SIP Trunk Profile

Profiles: Default

SIP Calling Number

SIP Protocol Field: Not Sent (default)

● Carrier can accept any number

○ Carrier can only accept Calling Number with minimum [ ] digits

○ Carrier can only accept assigned numbers as Calling Number

Calling Number can be accepted by Carrier

From	To

Use this as Calling Number if the Carrier cannot accept configured numbers

□ Send Caller Name □ Enable Standard Record-Route Header

Incoming DID Number field

● To Header ○ Request URI

Figure 12-7. SIP Trunk Profile dialog box

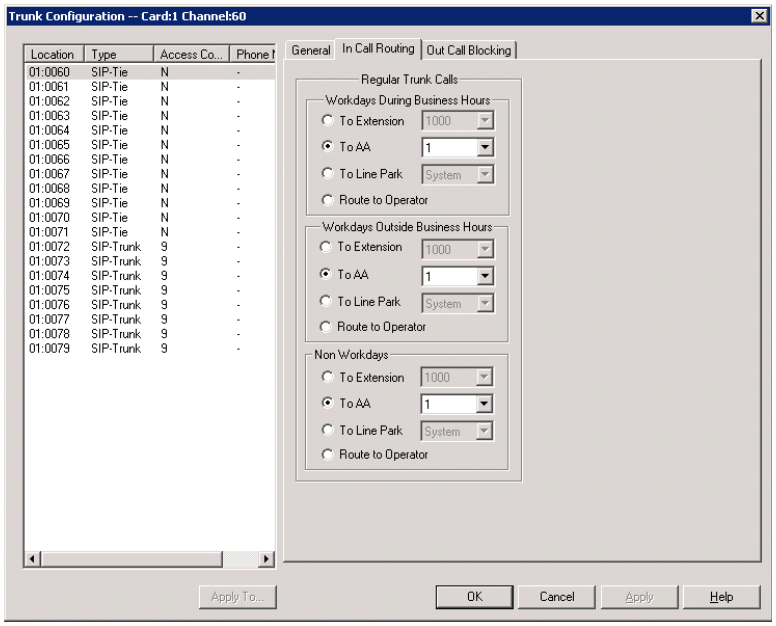
The fields in this dialog box are described in the following table.

Field	Description
SIP Protocol Field	**Not Sent** (default)—Do not send transmitted caller ID **FROM Header**—Send the caller ID using the SIP FROM header **P-Preferred Identity**—Send the caller ID using the SIP P-Preferred Identity header **P-Asserted Identity**—Send the caller ID using the SIP P-Asserted Identity header
Carrier can accept any number	This is the default.
Carrier can only accept Calling Number with minimum x digits	Enter the number of digits, then enter a calling number in the field below the table in case the carrier cannot accept configured numbers.
Carrier can only accept assigned numbers as Calling Number	If you select the this option, specify "assigned numbers" by clicking the **Add** button and entering the numbers. To edit or delete a number you added, select it and click the **Edit** or **Del** button. Enter a calling number in the field below the table in case the carrier cannot accept configured numbers.
Send Caller Name	Check to also send the caller name to callees.
Enable Standard Record-Route Header	Check this box if the SIP service provider uses SIP Record-Route and the SIP trunk cannot make or receive calls. If it already works, DO NOT CHECK or UNCHECK this box. [Service provider Bandwidth.com with Edgewater Route require this checked]

Field	Description
Incoming DID Number Field	When a call comes in, the SIP trunk uses **To Header** or **Request URI** as the DID/DNIS number

Incoming Call Routing

To set incoming call routing for a trunk, select the trunk on the **General** tab, then click the **In Call Routing** tab in the **Trunk Configuration** window. The trunk location appears in the title bar.



Trunk Configuration -- Card:1 Channel:60

Location	Type	Access Co...	Phone N
01:0060	SIP-Tie	N	-
01:0061	SIP-Tie	N	-
01:0062	SIP-Tie	N	-
01:0063	SIP-Tie	N	-
01:0064	SIP-Tie	N	-
01:0065	SIP-Tie	N	-
01:0066	SIP-Tie	N	-
01:0067	SIP-Tie	N	-
01:0068	SIP-Tie	N	-
01:0069	SIP-Tie	N	-
01:0070	SIP-Tie	N	-
01:0071	SIP-Tie	N	-
01:0072	SIP-Trunk	9	-
01:0073	SIP-Trunk	9	-
01:0074	SIP-Trunk	9	-
01:0075	SIP-Trunk	9	-
01:0076	SIP-Trunk	9	-
01:0077	SIP-Trunk	9	-
01:0078	SIP-Trunk	9	-
01:0079	SIP-Trunk	9	-

Regular Trunk Calls

Workdays During Business Hours
○ To Extension 1000
● To AA 1
○ To Line Park System
○ Route to Operator

Workdays Outside Business Hours
○ To Extension 1000
● To AA 1
○ To Line Park System
○ Route to Operator

Non Workdays
○ To Extension 1000
● To AA 1
○ To Line Park System
○ Route to Operator

Figure 12-8. Trunk Configuration, In Call Routing tab

Regular Trunk Calls

For each trunk—or using **Apply to** to apply the settings to multiple trunks—you can set routing for the three time periods defined in the **System Configuration** window, **Business Hours** tab (“Setting Business Hours” on page 39):

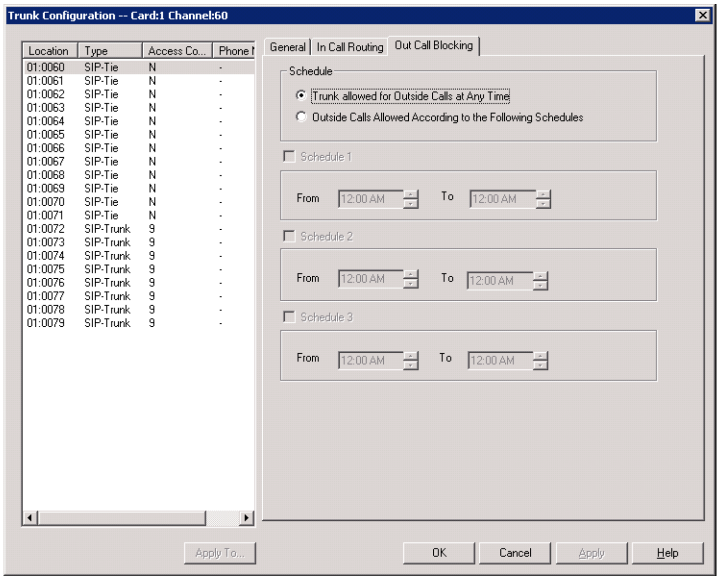
- During Business Hours
- Outside Business Hours
- Non Workdays

Within each of these three time slots, you have the following routing options for incoming calls:

- Route to an extension selected in the drop-down list
- Route to an auto attendant number selected in the drop-down list
- Route to a Line Park line selected in the drop-down list (see “Line Park Configuration” on page 147 for more detail)
- Route to the operator

Outgoing Call Blocking

To set outgoing call blocking for a trunk, select the trunk in the **General** tab, then click the **Out Call Blocking** tab in the **Trunk Configuration** window.



Location	Type	Access Co...	Phone
01:0060	SIP-Tie	N	-
01:0061	SIP-Tie	N	-
01:0062	SIP-Tie	N	-
01:0063	SIP-Tie	N	-
01:0064	SIP-Tie	N	-
01:0065	SIP-Tie	N	-
01:0066	SIP-Tie	N	-
01:0067	SIP-Tie	N	-
01:0068	SIP-Tie	N	-
01:0069	SIP-Tie	N	-
01:0070	SIP-Tie	N	-
01:0071	SIP-Tie	N	-
01:0072	SIP-Trunk	9	-
01:0073	SIP-Trunk	9	-
01:0074	SIP-Trunk	9	-
01:0075	SIP-Trunk	9	-
01:0076	SIP-Trunk	9	-
01:0077	SIP-Trunk	9	-
01:0078	SIP-Trunk	9	-
01:0079	SIP-Trunk	9	-

Schedule

● Trunk allowed for Outside Calls at Any Time

○ Outside Calls Allowed According to the Following Schedules

□ Schedule 1

From 12:00 AM To 12:00 AM

□ Schedule 2

From 12:00 AM To 12:00 AM

□ Schedule 3

From 12:00 AM To 12:00 AM

Figure 12-9. Trunk Configuration, Out Call Blocking tab

If you select **Trunk allowed for Outside Calls at Any Time**, call restrictions set in System Configuration, Outcall Routing, and Extension Configuration still apply to calls made on the trunk.

If you select **Outside Calls Allowed According to The Following Schedules**, you can then use the Schedule 1, 2, and 3 options to set up to three different time periods during which calls are allowed. You can use **Apply to** to apply the settings to multiple trunks.

CHAPTER

13

In Call Routing Configuration

In Call Routing rules determine how the system routes incoming trunk calls to various targets. The system's routing steps are as follows:

Step	Routing Process
1	Match DID number configured in extension, workgroup, or hunt group. If there is no match, go to the next step.
2	Match caller ID defined in the Caller ID Routing table. If there is a match and • today is a holiday, route the call according to the Holiday Profile's routing rules. • today is *not* a holiday, route the call according to business hour routing rules defined in the Caller ID Routing configuration. If there is no caller ID match, go to the next step.
3	Match DNIS number defined in the DNIS Routing table. If there is a match and • today is a holiday, route the call according to the Holiday Profile's routing rules. • today is *not* a holiday, route the call according to business hour routing rules defined in the DNIS Routing configuration. If there is no DNIS number match, go to the next step.
4	If today is a holiday, route the call according to the Holiday Profile configured for the trunk port that the call is coming in on. If today is *not* a holiday, route the call according to the business hours routing rules defined in the **In Call Routing** tab of the Trunk Configuration window.

The In Call Routing Configuration window lets you enter Caller ID and DNIS numbers into a routing table and set routing rules for a matched number.

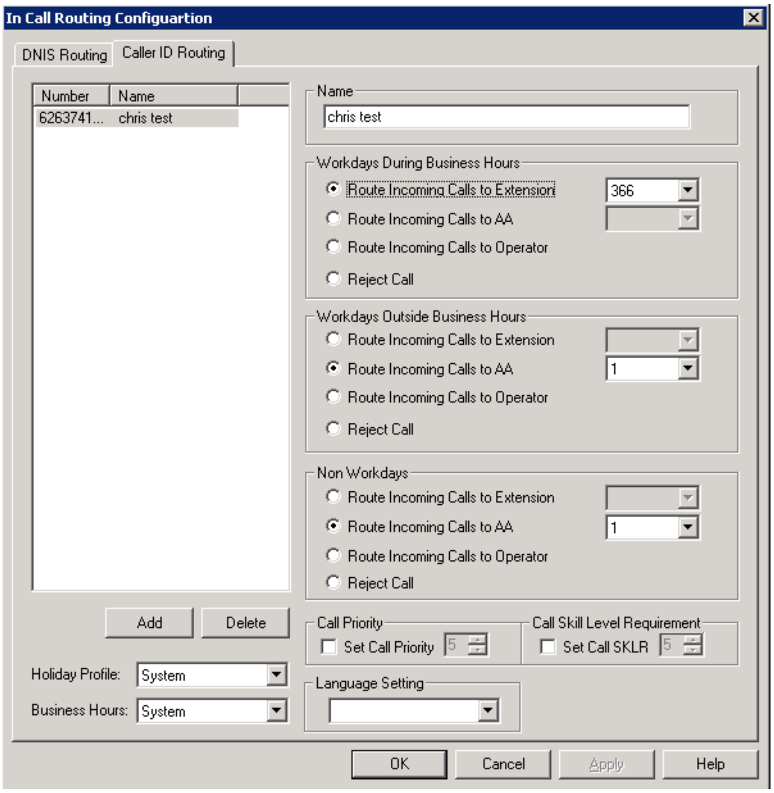
To configure In Call Routing, select **General > In Call Routing Configuration**.

Caller ID Routing

When an incoming call comes through a trunk with Caller ID, the system can route the call to the proper extension, to the auto attendant, or to the operator, based on the Caller ID number collected.

In order to locate an entry in the Caller ID table for an incoming call, a full match is required.

To access Caller ID routing, click the **Caller ID Routing** tab in the In Call Routing Configuration window.



Number	Name
6263741...	chris test

Name: chris test

Workdays During Business Hours
● Route Incoming Calls to Extension 366
○ Route Incoming Calls to AA
○ Route Incoming Calls to Operator
○ Reject Call

Workdays Outside Business Hours
○ Route Incoming Calls to Extension
● Route Incoming Calls to AA 1
○ Route Incoming Calls to Operator
○ Reject Call

Non Workdays
○ Route Incoming Calls to Extension
● Route Incoming Calls to AA 1
○ Route Incoming Calls to Operator
○ Reject Call

Call Priority: □ Set Call Priority 5

Call Skill Level Requirement: □ Set Call SKLR 5

Holiday Profile: System

Business Hours: System

Language Setting:

Figure 13-1. In Call Routing window, Caller ID Routing tab

Adding and Deleting Caller ID Route Entries

To add entries to the Caller ID routing table, click the **Add** button. In the dialog box that appears, type in a **Caller ID Number** and a descriptive **Caller ID Name**, then click **OK**.

The number and name entries have the following requirements:

- The **Caller ID Number** field allows only 0-9, "-" (hyphen), and "*" (asterisk). For example, both 5102529712 and 510-252-9712 are acceptable.
- The **Caller ID Name** is descriptive and optional; it can be used to remind you about the nature of the number and routing. For example, you might give the 2529712 number the name "Tech Support."

To delete an entry, select it in the Caller ID number list, then click **Delete**.

Configuring Caller ID Routing

After adding an entry, you configure it by first selecting it in the list. When you select an entry, its name and other defined attributes, if any, appear in the fields of the tab. You can edit any of these attributes.

For each number, you can set routing for three distinct time periods defined in the **Business Hours** tab (see "Setting Business Hours" on page 39):

- During Business Hours
- Outside Business Hours
- Non Workdays

Within each of these three time slots, you have the following routing options for incoming calls:

- Route to a particular extension selected in the drop-down list
- Route to a particular auto attendant selected in the drop-down list
- Route to the operator
- Reject call

Also, you can set additional routing attributes based on:

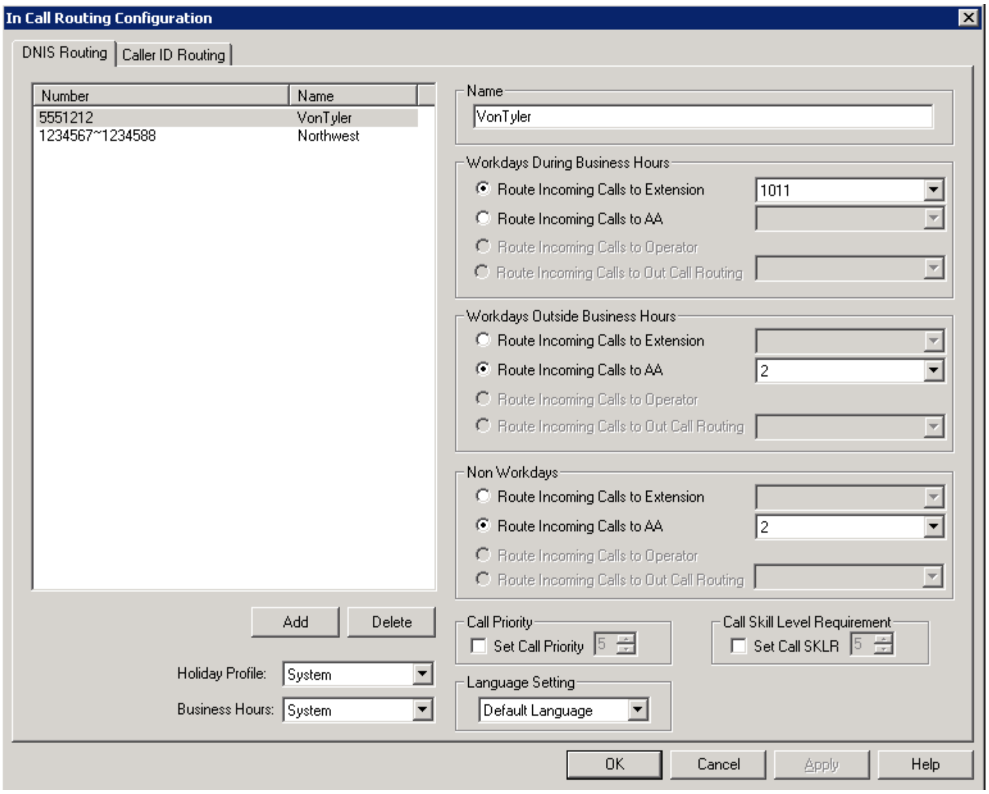
- **Holiday Profile**—routes incoming calls based on Holiday Profiles configured in System Configuration (see "Routing Calls on Holidays" on page 41)
- **Business Hours Profile**—routes incoming calls based on Business Hours Profiles configured in System Configuration (see "Setting Business Hours" on page 39). **During Business Hours**, **Outside Business Hours** and **Non Working Day** are defined and selected by Business Hours profile.
- **Set Call Priority**—lets you assign a call priority from 1-9 to the selected caller ID number. The highest priority is 1, the lowest priority is 9.
- **Set Call Skill Level Requirement**—for workgroup-directed calls. Lets you assign a skill level requirement from 1-9 to the selected caller ID number. This setting tells the system to match the call to an agent's skill level setting. (Setting an agent's skill level is explained in "Setting Up Skill Based Routing" on page 162.)
- **Language Setting**—lets you specify that callers who dialed from the selected caller ID will hear prompts in the language you set here. This field will have choices only if you added sets of prompts according to the instructions in "Multilingual Configuration" on page 75.

DNIS Routing

When an incoming call comes through a trunk with DNIS or DID numbers, the system can route the call to the proper extension, auto attendant or operator based on the DNIS or DID number collected.

In order to locate an entry in the DNIS table for an incoming call, a full match is required.

To access DNIS routing settings, click the **DNIS Routing** tab in the In Call Routing Configuration window.



Number	Name
5551212	VonTyler
1234567~1234588	Northwest

Name: VonTyler

Workdays During Business Hours

- ● Route Incoming Calls to Extension: 1011
- ○ Route Incoming Calls to AA
- ○ Route Incoming Calls to Operator
- ○ Route Incoming Calls to Out Call Routing

Workdays Outside Business Hours

- ○ Route Incoming Calls to Extension
- ● Route Incoming Calls to AA: 2
- ○ Route Incoming Calls to Operator
- ○ Route Incoming Calls to Out Call Routing

Non Workdays

- ○ Route Incoming Calls to Extension
- ● Route Incoming Calls to AA: 2
- ○ Route Incoming Calls to Operator
- ○ Route Incoming Calls to Out Call Routing

Call Priority: □ Set Call Priority 5

Call Skill Level Requirement: □ Set Call SKLR 5

Holiday Profile: System

Business Hours: System

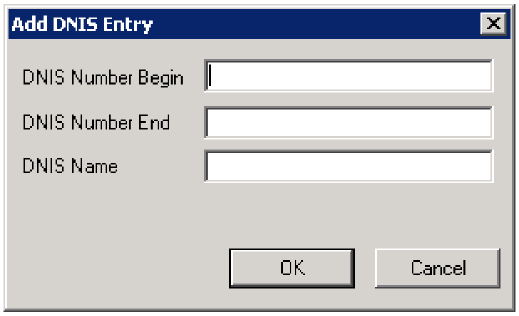
Language Setting: Default Language

Figure 13-2. In Call Routing window, DNIS Routing tab

Adding and Deleting DNIS Route Entries

To add entries to the DNIS routing table,

1. Click the **Add** button. The following dialog box opens:



DNIS Number Begin:

DNIS Number End:

DNIS Name:

One DNIS entry can cover a range of numbers. Type the beginning number in the range and the end number.

Figure 13-3. Add DNIS Entry dialog box

2. Type a DNIS number in the **DNIS Number Begin** field. The same number appears in the **DNIS Number End** field.
3. If this entry is to cover a range of DNIS numbers, edit the second field to indicate the last number in the range. If the entry is for one number only, leave the field alone, or you can delete the end number.

4. Enter a descriptive **DNIS Name**, then click **OK**.

The number and name entries have the following requirements:

- The **DNIS Number** must be the numbers 0–9 (the hyphen is not accepted in this dialog box). For example, 2529876 is an acceptable entry, but 252-9876 is not.
- The **DNIS Name** is descriptive and optional; it can be used to remind you about the nature of the number and routing. For example, you might give the 2529876 number the name "Tech Support."

To delete an entry, select it in the DNIS number list, then click **Delete**.

Configuring DNIS Routing

After adding an entry, you configure it by first selecting it in the list. When you select an entry, its name and other defined attributes, if any, appear in the fields of the tab. You can edit any of these attributes.

For each number, you can set routing for three distinct time periods defined in the **Business Hours** tab (see "Setting Business Hours" on page 39):

- During Business Hours
- Outside Business Hours
- Non Workdays

Within each of these three time slots, you have the following routing options for incoming calls:

- Route to a particular extension selected in the drop-down list
- Route to a particular auto attendant selected in the drop-down list
- Route to the operator
- Route incoming calls to out call routing

Also, you can set additional routing attributes based on:

- **Holiday Profile**—routes incoming calls based on Holiday Profiles configured in the System Configuration window (see "Routing Calls on Holidays" on page 41)
- **Business Hours Profile**—routes incoming calls based on Business Hours Profiles configured in the System Configuration window (see "Setting Business Hours" on page 39). **During Business Hours**, **Outside Business Hours** and **Non Working Day** are defined and selected by the Business Hours profile.
- **Set Call Priority**—lets you assign a call priority from 1-9 to the selected DNIS number. The highest priority is 1, the lowest priority is 9.
- **Set Call SKLR**—for workgroup-directed calls. Lets you assign a skill level requirement from 1-9 to the selected DNIS number. This setting tells the system to match the call to an agent's skill level setting. (Setting an agent's skill level is explained in "Setting Up Skill Based Routing" on page 162.)
- **Language Setting**—lets you specify that callers who dialed the selected number will hear prompts in the language you set here. This field will have choices only if you added sets of prompts according to the instructions in "Multilingual Configuration" on page 75.

CHAPTER

14

Out Call Routing Configuration

There are two ways to initiate outbound dialing:

- **Using the trunk access code**
  The trunk access code is easy to configure and use. However, it does not have the capability to resolve complicated dialing situations.
- **Using the route access code**
  Using the route access code with the Out Call Routing table can resolve the following complicated dialing situations:
  - Multiple 10-digit dialing area codes.
  - Both 10-digit and 11-digit dialing in the same area code.
  - Multiple carriers providing trunks for different purposes. For example, you may have a local carrier provide trunks for local calls only and a long distance carrier provide trunks that can accept only long distance dialing.
  - Block certain dialing patterns by creating an exceptions list.
  - Assist system Zoomerang and client application dialing, for example, MaxAgent. For example, dialing from MaxAgent will carry 11 digits and require the system to remove a digit before making a call to the carrier if it is a 10-digit dialing area.
  - Divide trunks with the same characteristics into multiple routes and prioritize them when assigning routes on the **Default Routes** tab or on the **Dialing Pattern** tab of the Out Call Routing Configuration window.

When a user dials an outside number using the route access code, the system performs the following tasks:

- Compares the dialed number with entries in the **Dialing Pattern** table. If there is a match, the system uses the route assigned to the dialing pattern to make the outbound call. The route assigned to the special dialing pattern may have a digit manipulation rule to add or remove digits from the dialed number.
- If there is no match in the **Dialing Pattern** table, the system examines the digits to determine if the call is a local, long distance, international, or emergency call. The routes defined in the **Default Routes** tab are used to process the call.

Configuring Out Call Routing

To configure out call routing, select **General > Out Call Routing Configuration**. The following configuration steps may help you configure out call routing correctly.

1. Before you configure Out Call Routing, make sure a route access code is configured in the System Configuration window, **Number Plan** tab. If you have a problem changing a first-digit assignment in the **Number Plan** tab to a route access code, you may need to set the **Access Code** in the Trunk Configuration window for all trunks to **None**.
2. Create a route and assign trunks to the route.
3. Assign routes as Default Routes so that regular 7-digit, 11-digit, international, and emergency calls will go through.
4. Solve a complicated dialing situation by adding an entry into the **Dialing Pattern** table and assigning a route to the specific dialing pattern.
5. If the dialing pattern requires adding or removing digits, you may need to edit the **Digit Manipulation** on the **Route Definition** tab to solve the problem. Repeat steps 4 and 5 until all complicated dialing patterns are entered and configured properly.
6. If you would like to block a specific dialing pattern, add the dialing pattern and check **Disallow this dialing pattern** check box.

WARNING! Make sure the default 911 route is configured to a route that can accept 911 calls. (See Figure 14-3, “Out Call Routing Configuration, Default Routes tab".) Failure to do so may cause failure of direct 911 dialing. If you do not want a user to call 911 directly because of too many 911 dialing errors, you can leave the 911 route not configured. In this case, you need to let all extension users know that they need to dial 9+911 to call emergency service. A proper warning sticker on the phone to notify employees about 9+911 dialing would be a good practice.

Some configuration examples are provided at the end of the chapter. Please use them as a reference to help you configure your dialing pattern correctly.

Working with Route Definitions

A route definition consists of a route name and group of trunks, listed in the order that the system will use for outgoing calls.

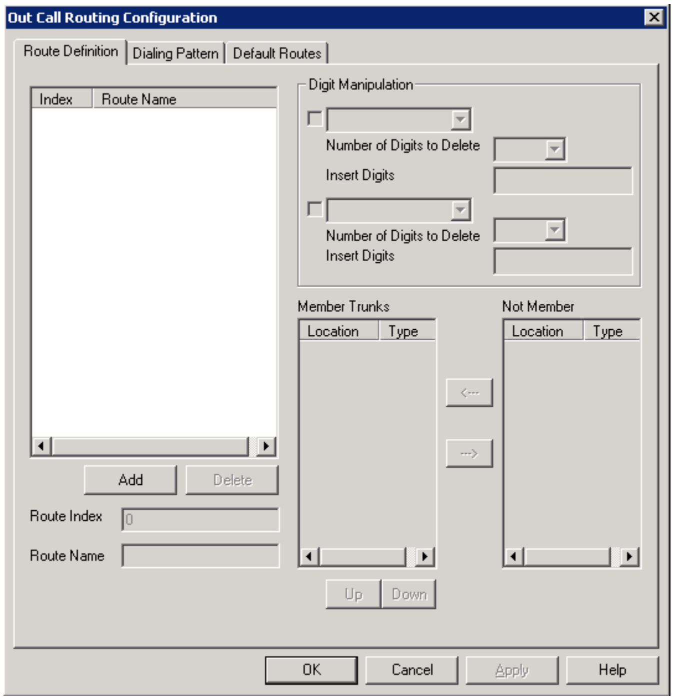
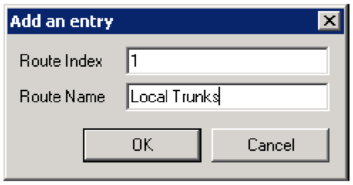


Figure 14-1. Out Call Routing Configuration, **Route Definition** tab

Parameter	Description
Route Index	For identification purposes only.
Route Name	Description of the route (maximum 30 characters).
Digit Manipulation	You can insert or delete digits from the dialed number. See configuration samples to learn how to use digit manipulation in different situations. **Insert to Head**: Insert a string of digits in front of the dialed number. **Delete from Head**: Remove a string of digits from the beginning of the dialed number.
Member Trunks	Displays the trunks assigned to the selected route. The order in which member trunks are added determines the order in which the trunks are used by the system when making an outbound call (the first trunk listed is used first, and so forth).
Not Member	Displays all trunks that are not assigned to the selected route.

Creating a Route

1. Click **Add** under the route definition list.



Add an entry

Route Index 1

Route Name Local Trunks

Figure 14-2. Add route entry dialog box

2. Type in a name and index number, and click **OK**.
3. To add trunks to the route, select trunks from the **Not Member** list and use the <-- button to move selected trunks to the **Member Trunks** list.
4. Use the **Up** and **Down** buttons to change the position of a trunk in the **Member Trunks** list. This is the order in which trunks are accessed.
5. Click **Apply**.

To delete a route

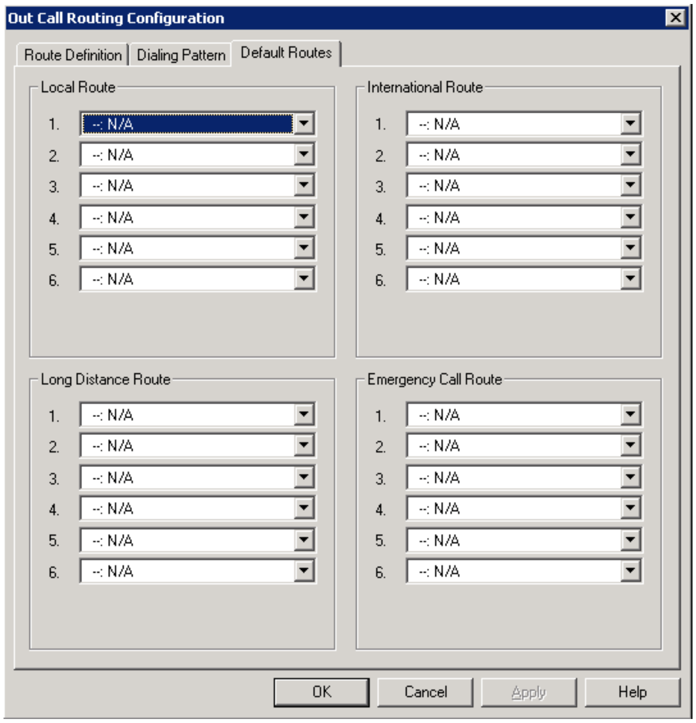
Select the route you want to delete, and click the **Delete** button.

Setting Default Routes

You can set default routes for four types of outgoing calls: **local, long distance, international,** and **emergency**.

WARNING! It is important that you set up default routes **right after routes are defined**. Failing to do so will cause outbound dialing failure.

Click the **Default Routes** tab in the **Out Call Routing Configuration** window to configure default routes.



Local Route

1. --: N/A
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

International Route

1. --: N/A
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

Long Distance Route

1. --: N/A
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

Emergency Call Route

1. --: N/A
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

For each type of call, the system will use trunks specified in the “1” field, if available, otherwise use trunks in the “2” field, and so on.

Figure 14-3. Out Call Routing Configuration, **Default Routes** tab

Working on Dialing Patterns

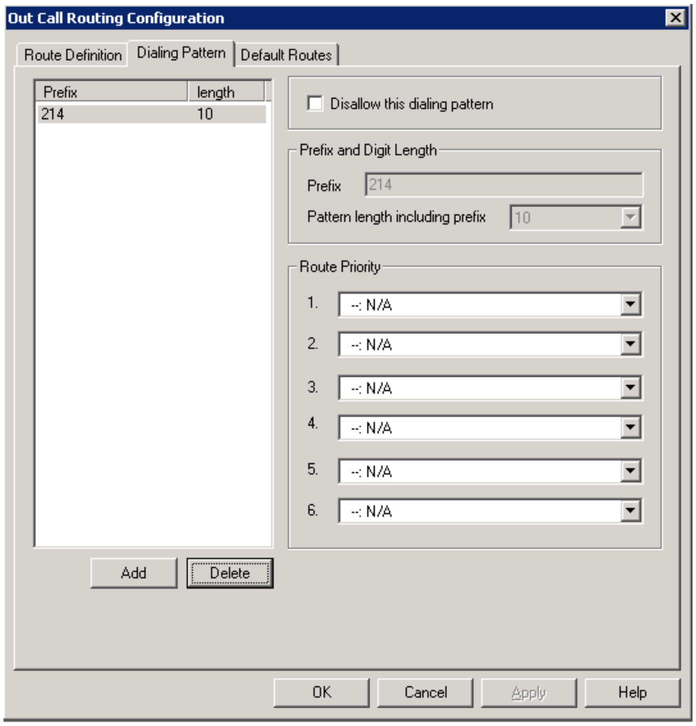
If your system is using a route access code, most likely you have one of the following situations:

- Your area may have multiple 10-digit dialing area codes.
- Your area may have both 10-digit and 1+10 digit dialing in a same area code.
- You would like to block a dialing pattern in addition to system restriction setting.

Dialing patterns are exceptions. If you can, minimize the number of dialing pattern entries. Most companies don’t need to create dialing patterns.

To create a dialing pattern,

1. Click the **Dialing Pattern** tab on the Out Call Routing Configuration window.



Prefix	length
214	10

☐ Disallow this dialing pattern

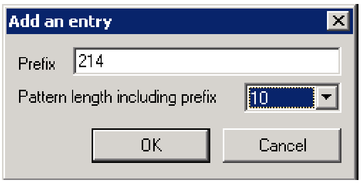
Prefix: 214

Pattern length including prefix: 10

1. --: N/A
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

Figure 14-4. Out Call Routing Configuration, **Dialing Pattern** tab

2. Click the **Add** button.



Prefix: 214

Pattern length including prefix: 10

Figure 14-5. Add dialing pattern dialog box

3. Type the prefix and pattern length, and click **OK**.
4. Assign routes to this prefix by selecting routes from the drop-down lists in the Route Priority section of the **Dialing Pattern** tab.
5. If this is a restricted number or pattern, skip step 4 and check the **Disallow this dialing pattern** check box.

To delete a dialing pattern

Select the pattern you want to delete, and click the **Delete** button.

Dialing pattern configuration tips

- If a dialing pattern has multiple routes assigned to it, the system will try to use the first route configured to process the call that has this dialing pattern. If the first route is busy or not in service, the system will use the second route, and so on.

- If a dialing pattern requires the system to add or remove digits, a route with digit manipulation configuration needs to be set up correctly. This means that you may need to have the same group of trunks belong to different routes. Each route may have a different digit manipulation rule.
- If you are using dialing pattern to restrict outgoing calls, you need to be aware of the following system implementations:
    - The system first checks to see if the number is blocked for this extension (a setting in the Extension Configuration window, **Restriction** tab).
    - The system then checks the System Configuration **Call Restriction** tab settings to see if this number is blocked by the system.
    - The system then checks the **Dialing Pattern** configuration, and if a specific number or pattern is not blocked, the system will dial the number through a proper route.

  In other words, if extension and system call restrictions are not blocking a number or pattern, you can use Out Call Routing to build restriction rules to block numbers or patterns.

CHAPTER

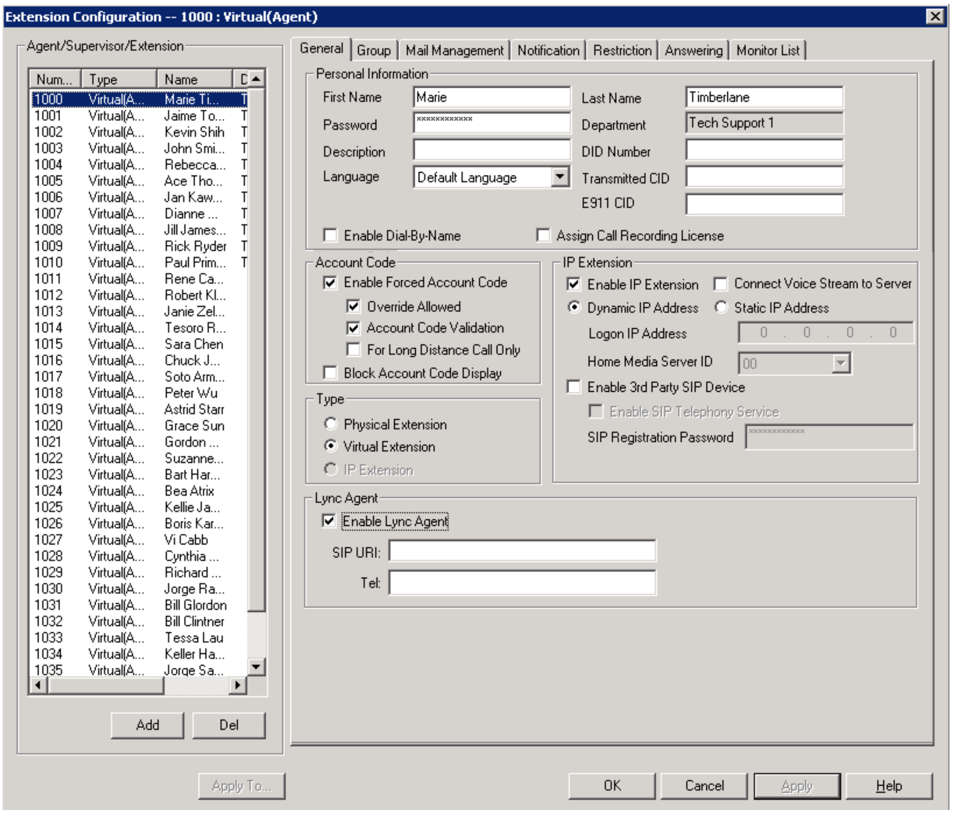
15

Extension Configuration

The Extension Configuration window provides for creating extensions and setting their attributes. To open the Extension Configuration window, do one of the following:

- Click the **Extension Configuration** button on the toolbar.
- Select **General > Extension Configuration**.

Note: To set up an application extension, see “Application Extension Configuration” on page 87.



Extension Configuration -- 1000 : Virtual(Agent)

Agent/Supervisor/Extension

Num...	Type	Name	D
1000	Virtual(A...	Marie Ti...	T
1001	Virtual(A...	Jaime To...	T
1002	Virtual(A...	Kevin Shih	T
1003	Virtual(A...	John Smi...	T
1004	Virtual(A...	Rebecca...	T
1005	Virtual(A...	Ace Tho...	T
1006	Virtual(A...	Jan Kaw...	T
1007	Virtual(A...	Dianne ...	T
1008	Virtual(A...	Jill James...	T
1009	Virtual(A...	Rick Ryder	T
1010	Virtual(A...	Paul Prim...	T
1011	Virtual(A...	Rene Ca...	
1012	Virtual(A...	Robert Kl...	
1013	Virtual(A...	Janie Zel...	
1014	Virtual(A...	Tesoro R...	
1015	Virtual(A...	Sara Chen	
1016	Virtual(A...	Chuck J...	
1017	Virtual(A...	Soto Arm...	
1018	Virtual(A...	Peter Wu	
1019	Virtual(A...	Astrid Starr	
1020	Virtual(A...	Grace Sun	
1021	Virtual(A...	Gordon ...	
1022	Virtual(A...	Suzanne...	
1023	Virtual(A...	Bart Har...	
1024	Virtual(A...	Bea Atrix	
1025	Virtual(A...	Kellie Ja...	
1026	Virtual(A...	Boris Kar...	
1027	Virtual(A...	Vi Cabb	
1028	Virtual(A...	Cynthia ...	
1029	Virtual(A...	Richard ...	
1030	Virtual(A...	Jorge Ra...	
1031	Virtual(A...	Bill Glordon	
1032	Virtual(A...	Bill Clintner	
1033	Virtual(A...	Tessa Lau	
1034	Virtual(A...	Keller Ha...	
1035	Virtual(A...	Jorge Sa...	

Personal Information

First Name: Marie
Last Name: Timberlane
Password: ************
Department: Tech Support 1
Description:
DID Number:
Language: Default Language
Transmitted CID:
E911 CID:

□ Enable Dial-By-Name
□ Assign Call Recording License

Account Code

☑ Enable Forced Account Code
☑ Override Allowed
☑ Account Code Validation
□ For Long Distance Call Only
□ Block Account Code Display

Type

○ Physical Extension
● Virtual Extension
○ IP Extension

IP Extension

☑ Enable IP Extension
□ Connect Voice Stream to Server
● Dynamic IP Address
○ Static IP Address
Logon IP Address: 0 . 0 . 0 . 0
Home Media Server ID: 00
□ Enable 3rd Party SIP Device
□ Enable SIP Telephony Service
SIP Registration Password: ************

Lync Agent

☑ Enable Lync Agent
SIP URI:
Tel:

Figure 15-1. Extension Configuration window

Using the Apply To Button

A change you make to an extension can often be applied to one or more other extensions by using the **Apply To** button.

Clicking the **Apply To** button pops up a list of all extensions to which the change can apply. Select the extensions to which you want to apply the change (all are selected, by default). Use the **Shift** or **Ctrl** keys to select several extensions.

The **Apply To** button is disabled unless a change you made can be applied to other extensions. When you use the button to apply changes to multiple extensions, it works on only those changed attributes that can be applied.

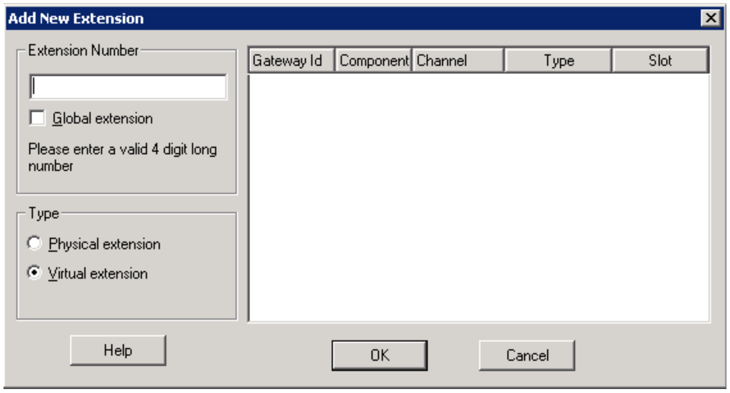
Setting up Extensions

Set up new extensions in the Extension Configuration window.

To create MaxACD agent extensions that correspond to Microsoft Lync Client users, set up users in Microsoft Lync first. Then configure corresponding extensions in MaxACD.

To add an extension:

1. Click the **Add** button below the **Agent/Supervisor/Extension** list.



Add New Extension

Extension Number

□ Global extension

Please enter a valid 4 digit long number

Type

○ Physical extension

● Virtual extension

Figure 15-2. Add New Extension dialog box

2. Type in an **Extension Number**.

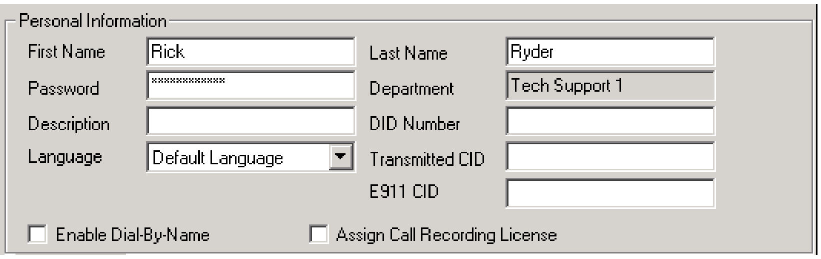
   The number must begin with a number assigned to be used for extensions, and it must be the length assigned to extensions, both of which are set on the **Number Plan** tab in the System Configuration window, as described in “Setting a System Number Plan” on page 35.

3. In the Type panel, select **Virtual**. Click **OK**.

After you create an extension, you can set basic attributes on the Extension Configuration **General** tab. These attributes are discussed below.

Setting Personal Information

The top section of the **General** tab is for personal Information.



Personal Information

First Name: Rick

Last Name: Ryder

Password: ************

Department: Tech Support 1

Description:

DID Number:

Language: Default Language

Transmitted CID:

E911 CID:

□ Enable Dial-By-Name

□ Assign Call Recording License

Figure 15-3. General tab, top section

- **First Name** and **Last Name** of the extension user, each with a maximum of 32 characters. First and last names *must match exactly* with their Lync Client user counterparts when setting up a MaxACD agent.

  Note: Only letters can be used for these fields. Inputting numbers or symbols (such as "#", "*", "/", "-" are blocked, so as not to conflict with Dial by Name (#34) and other feature codes.

- **Password** for the extension user. The default is the system default password set on the **Number Plan** tab in the System Configuration window.

  A valid password must be 4 to 8 digits (numbers or letters A-Z) in length and cannot be the same as its extension number. Basic password patterns, such as repeated digits (1111), consecutive digits strings (1234), or digits that match the extension (Ext. **101** using **101**2, 9**101**, **101**01, and so on) are not allowed. The letters map to numbers as follows:

Numbers	Letters	Numbers	Letters
2	A, B, C, a, b, c	6	M, N, O, m, n, o
3	D, E, F, d, e, f	7	P, Q, R, S, p, q, r, s
4	G, H, I, g, h, i	8	T, U, V, t, u, v
5	J, K, L, j, k, l	9	W, X, Y, Z, w, x, y, z

- **Department**—Departments can be defined and extensions can be assigned to a department by using Enterprise Manager. When this is done, the department is displayed here.

- **Description**—Optional descriptive information such as cubicle number or job title.

- **DID Number**—If this extension is being set up to correspond to a Lync Client user, fill in the same DID as the Lync user.

  Each extension can be assigned a DID number. This number does not have a fixed length, but the length must be long enough (range 2–16) for the system to match the DID incoming call. If you configure a 10-digit DID number and inbound digital trunks only receive 4 digits, the last 4 digits of the DID number configured will be matched.

- **Transmitted CID**—Each extension number can be assigned a caller ID number. When an outgoing call is made by this extension, the caller ID number entered in this field will be transmitted to the receiving caller.

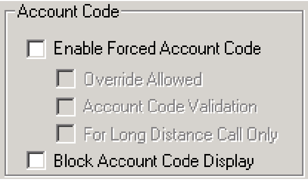
- **E911 CID**—A number entered in this field will be transmitted as the caller ID for 911 calls made by this extension.

Note: If a number is not entered in the **E911 CID** field, the **Transmitted CID** is transmitted as the caller ID for 911 calls made by this extension.

- **Language**—Sets the language the extension user will hear for voice mail and system prompts. If voice mail and system phrases have been translated into other languages and properly added to the C:\PostOffice\Phrases directory, the languages will be selectable from the **Language** drop-down list. (See "Multilingual Configuration" on page 75 for information on adding translated prompts to the MaxACD system).
- **Enable Dial-By-Name—**Select this box to allow incoming callers to search the extension list by employee name for this extension.
- **Assign Call Recording License—**Assigns this extension a call recording license.

Account Code

These settings determine how callers use any account codes you have established when making outgoing trunk calls.



Account Code

☐ Enable Forced Account Code

☐ Override Allowed

☐ Account Code Validation

☐ For Long Distance Call Only

☐ Block Account Code Display

Figure 15-4. Account code dialog box

For information on creating account/code associations, see "Creating Account Codes" on page 45.

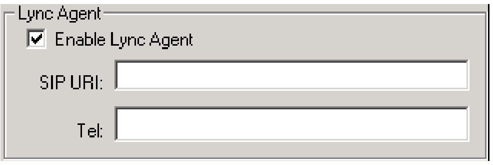
- **Enable Forced Account Code**—Forces the user to enter an account code.
- **Override Allowed**—Prompts the user to enter an account code, or the user can press # to bypass the account code.
- **Account Code Validation**—Forces the user to enter a valid account code.
- **For Long Distance Call Only**—The system determines if an outgoing call starts with a long distance or international prefix. If it does, the call will require an account code.
- **Block Account Code Display**—The account code table will not be displayed when the user tries to tag the account from MaxAgent. This prevents the user from seeing account codes they do not need to see.

IP Extension Configuration

Check **Enable IP Extension** and select **Dynamic IP Address**.

Lync Agent

Check the **Enable Lync Agent** check box if this extension is to be a MaxACD agent that corresponds to a Lync Client user.



Lync Agent

☑ Enable Lync Agent

SIP URI:

Tel:

Figure 15-5.   Enable Lync Agent dialog box

1. Enter the Lync Client user’s primary SIP URI that the user uses to log in.
2. In the **Telephone** field, enter the E164 phone number of the Lync Client user.

Configuring Group Options for an Extension

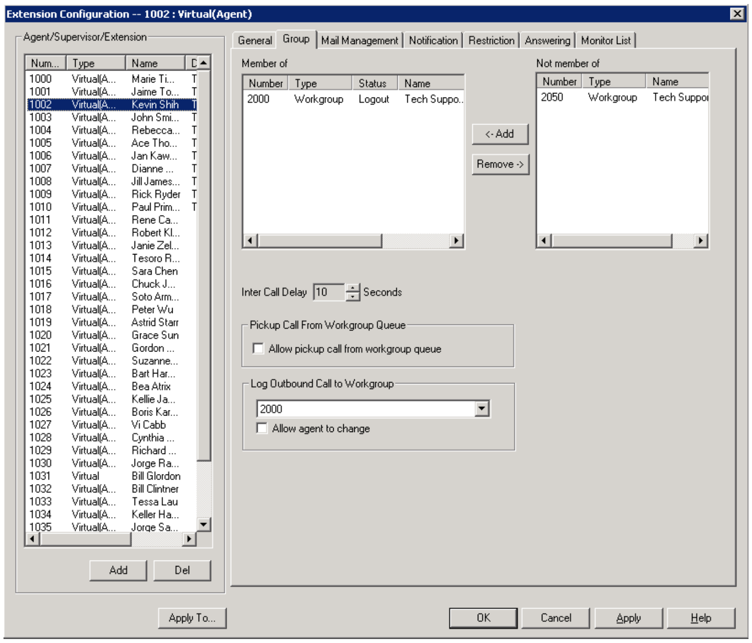
In the Extension Configuration window, **Group** tab, you can see the workgroups to which an extension is assigned, and you can change those assignments. Workgroups are created in the Workgroup Configuration window (see “Establishing Workgroup Membership” on page 159). Group members are assigned in those configuration windows, as well.

Once a workgroup is established, use the Extension Configuration window, **Group** tab, to configure workgroup options for an individual agent extension.

You can assign an extension to and remove an extension from a workgroup in the Extension Configuration window too. To assign an extension to a workgroup, the extension must be designated as an agent extension. This is done on the **General** tab of Extension Configuration (check the **Enable Lync Agent** check box and fill in the SIP URI and telephone number).

To configure group options for an individual extension

1. Select the extension number from the **Agent/Supervisor/Extension** list in the Extension Configuration window. The extension number and type appear in the title bar of the window.
2. Click the **Group** tab. You see a list of groups the agent is a member of and a list of groups the agent is not a member of. If the extension is not an agent, no workgroups are shown.



Agent/Supervisor/Extension

Num...	Type	Name	D
1000	Virtual(A...	Marie Ti...	T
1001	Virtual(A...	Jaime To...	T
1002	Virtual(A...	Kevin Shih	T
1003	Virtual(A...	John Smi...	T
1004	Virtual(A...	Rebecca...	T
1005	Virtual(A...	Ace Tho...	T
1006	Virtual(A...	Jan Kaw...	T
1007	Virtual(A...	Dianne ...	T
1008	Virtual(A...	Jill James...	T
1009	Virtual(A...	Rick Ryder	T
1010	Virtual(A...	Paul Prim...	T
1011	Virtual(A...	Rene Ca...	
1012	Virtual(A...	Robert Kl...	
1013	Virtual(A...	Janie Zel...	
1014	Virtual(A...	Tesoro R...	
1015	Virtual(A...	Sara Chen	
1016	Virtual(A...	Chuck J...	
1017	Virtual(A...	Soto Arm...	
1018	Virtual(A...	Peter Wu	
1019	Virtual(A...	Astrid Starr	
1020	Virtual(A...	Grace Sun	
1021	Virtual(A...	Gordon ...	
1022	Virtual(A...	Suzanne...	
1023	Virtual(A...	Bart Har...	
1024	Virtual(A...	Bea Atrix	
1025	Virtual(A...	Kellie Ja...	
1026	Virtual(A...	Boris Kar...	
1027	Virtual(A...	Vi Cabb	
1028	Virtual(A...	Cynthia ...	
1029	Virtual(A...	Richard ...	
1030	Virtual(A...	Jorge Ra...	
1031	Virtual	Bill Glordon	
1032	Virtual(A...	Bill Clintner	
1033	Virtual(A...	Tessa Lau	
1034	Virtual(A...	Keller Ha...	
1035	Virtual(A...	Jorge Sa...	

Member of

Number	Type	Status	Name
2000	Workgroup	Logout	Tech Suppo...

Not member of

Number	Type	Name
2050	Workgroup	Tech Suppor

Inter Call Delay 10 Seconds

Pickup Call From Workgroup Queue

☐ Allow pickup call from workgroup queue

Log Outbound Call to Workgroup

2000

☐ Allow agent to change

Figure 15-6. Extension Configuration window, Group tab

To assign a group to the selected extension

1. On the **Group** tab, click the group number in the **Not Member** list.
2. Click the **Add** button to move it to the **Member** list.

Note: If a workgroup is configured to Ring All Available Members, the maximum number of members is 20. See “Setting Call Handling Options” on page 171 for details.

To remove a group assigned to an extension

1. Click the group number in the **Member** list.
2. Click the **Remove** button. The group moves to the **Not Member** list.

Note: You can use **Shift**+click and **Ctrl**+click to select more than one group.

Setting Wrap-up Time

You can set the Wrap-up Time for the selected physical agent extension. This option doesn’t appear for a virtual extension or a non-agent extension. Wrap-up time is a system delay between the time an agent finishes a workgroup call and the time the next call is routed to the extension. It gives the agent time to finish up with notes, prepare for the next call, log out of the group, or click the “Wait” button in MaxAgent. You can set a wrap-up time of up to 29 minutes, 59 seconds.

Setting Inter Call Delay

This configuration applies only to calls waiting in queue. The inter-call delay can create a time delay before the next workgroup call *in queue* rings the extension after the extension finishes one of the following activities:

- Makes an internal or outbound call

- Receives a direct inbound call
- Accesses voice mail

It is possible that an agent may execute one of the above activities during the wrap-up period after finishing a workgroup call. The following rules govern which delay timer will take effect:

- If wrap-up time is still active, the inter-call delay will be ignored.
- If wrap-up time is expired when one of the above activities is completed, the inter-call delay will be applied. The system will not pass a workgroup call to an agent until inter-call delay is expired.

To set the extension Inter Call Delay time

1. Check the **Inter Call Delay** check box.
2. Using the drop-down lists, select the seconds for the delay.

Picking Up a Call from the Workgroup Queue

Check **Allow pickup call from workgroup queue** to allow a MaxAgent user to pick up a call from the workgroup the agent belongs to. The agent needs to be in the log-in state to be able to pick up a call from the queue.

Logging Outbound Workgroup Calls

You can assign an agent to an outgoing workgroup, which is useful for call detail reporting and workgroup statistics. All calls made by the agent while logged into the workgroup will be tracked as calls from the workgroup. The agent's outgoing workgroup can be assigned to any workgroup of which he is a member.

To set an agent's outgoing workgroup

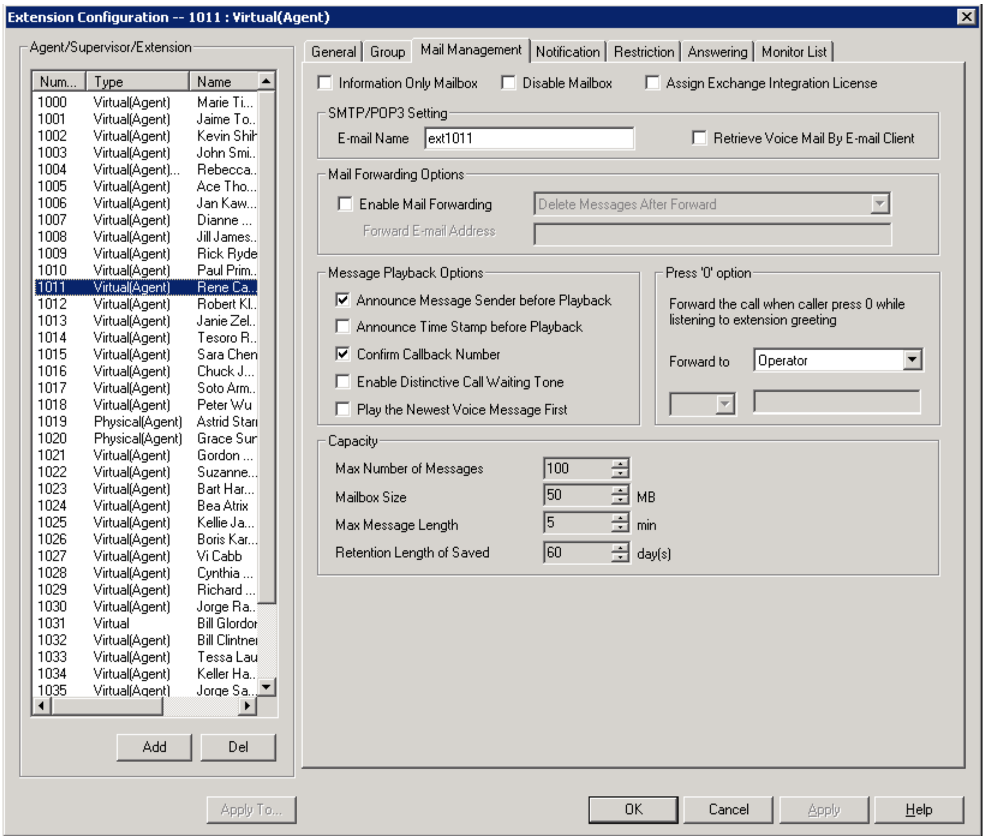
In the **Log Outbound Call to Workgroup** field, use the drop-down list to choose a workgroup from among the workgroups the agent belongs to. If the **Allow agent to change** check box is selected, the agent can change the outgoing workgroup from MaxAgent.

When a user is first assigned to a workgroup, it is set as their default outgoing workgroup and remains so no matter how many workgroups the user is subsequently assigned to. If an agent is unassigned from their outgoing workgroup, the outgoing workgroup is automatically set to N/A.

Setting Mailbox Options

The **Mail Management** settings define how voice messages are handled for an extension: whether the mailbox is information only or is full-featured, how messages are announced and processed, and how much capacity is allotted to message storage.

To work with mailbox settings, select the extension number you want to work with from the **Agent/Supervisor/Extension** list, then click the **Mail Management** tab.



Extension Configuration -- 1011 : Virtual(Agent)

Agent/Supervisor/Extension

Num...	Type	Name
1000	Virtual(Agent)	Marie Ti...
1001	Virtual(Agent)	Jaime To..
1002	Virtual(Agent)	Kevin Shih
1003	Virtual(Agent)	John Smi..
1004	Virtual(Agent)...	Rebecca..
1005	Virtual(Agent)	Ace Tho...
1006	Virtual(Agent)	Jan Kaw...
1007	Virtual(Agent)	Dianne ...
1008	Virtual(Agent)	Jill James..
1009	Virtual(Agent)	Rick Ryde
1010	Virtual(Agent)	Paul Prim..
1011	Virtual(Agent)	Rene Ca...
1012	Virtual(Agent)	Robert Kl..
1013	Virtual(Agent)	Janie Zel..
1014	Virtual(Agent)	Tesoro R...
1015	Virtual(Agent)	Sara Chen
1016	Virtual(Agent)	Chuck J...
1017	Virtual(Agent)	Soto Arm..
1018	Virtual(Agent)	Peter Wu
1019	Physical(Agent)	Astrid Stan
1020	Physical(Agent)	Grace Sur
1021	Virtual(Agent)	Gordon ...
1022	Virtual(Agent)	Suzanne...
1023	Virtual(Agent)	Bart Har...
1024	Virtual(Agent)	Bea Atrix
1025	Virtual(Agent)	Kellie Ja...
1026	Virtual(Agent)	Boris Kar...
1027	Virtual(Agent)	Vi Cabb
1028	Virtual(Agent)	Cynthia ...
1029	Virtual(Agent)	Richard ...
1030	Virtual(Agent)	Jorge Ra..
1031	Virtual	Bill Glordon
1032	Virtual(Agent)	Bill Clintner
1033	Virtual(Agent)	Tessa Lau
1034	Virtual(Agent)	Keller Ha..
1035	Virtual(Agent)	Jorge Sa...

☐ Information Only Mailbox ☐ Disable Mailbox ☐ Assign Exchange Integration License

SMTP/POP3 Setting

E-mail Name: ext1011 ☐ Retrieve Voice Mail By E-mail Client

Mail Forwarding Options

☐ Enable Mail Forwarding: Delete Messages After Forward

Forward E-mail Address:

Message Playback Options

☑ Announce Message Sender before Playback

☐ Announce Time Stamp before Playback

☑ Confirm Callback Number

☐ Enable Distinctive Call Waiting Tone

☐ Play the Newest Voice Message First

Press '0' option

Forward the call when caller press 0 while listening to extension greeting

Forward to: Operator

Capacity

Max Number of Messages: 100

Mailbox Size: 50 MB

Max Message Length: 5 min

Retention Length of Saved: 60 day(s)

Figure 15-7. Extension Configuration, Mail Management tab

Setting an Information-Only Mailbox

You can check the **Information Only Mailbox** check box to set extension mailboxes to Information Only, then click **Apply to** to set one or more extension mailboxes.

An Information Only mailbox allows callers to listen to customized recorded announcements. This mailbox does not take messages from the caller.

Disabling a Mailbox

When you disable a mailbox, a special greeting is played to announce that this mailbox is not accepting new messages.

Assign Exchange Integration License

Check this check box if the selected extension is to be integrated with Microsoft Exchange.

SMTP/POP3 Setting

- **E-mail Name**—the user's e-mail name without the @domain. The default e-mail name is ext*[extension number],* that is, the letters "ext" followed by the extension number. For example, the default e-mail name for extension 2497 would be **ext2497**.
- **Retrieve Voice Mail by E-mail Client**—selected, this sends voice mail to the user's e-mail as an attachment.

Mail Forwarding Options

- **Enable Mail Forwarding**—selected, the user's e-mail will be forwarded to the e-mail address you specify in the **Forward E-mail Address** box. The address should be a full address, including the domain (for example, *jsmith@thecompany.com*).

  If you enable mail forwarding, you also specify what you want done with the original messages after they have been forwarded. In the drop down list you can choose to:

  - Delete Messages after Forward
  - Keep the Messages as New
  - Keep Messages as Saved

Setting Message Playback Options

You can use the following check boxes to turn on or off options for listening to playback of recorded messages. These options apply to both new messages and saved messages, and they can be applied to multiple extensions using **Apply to**.

Parameter	Description
Announce Message Sender Before Playback	Selected, the user hears the *type* of the message sender (internal or outside) before listening to recorded messages.
Announce Time Stamp Before Playback	Selected, the user hears the timestamp (time and date) of each message before playback.
Confirm Callback Number	Selected, the system reads back the caller's number and asks the caller to confirm.
Enable Distinctive Call Waiting Tone	Selected, the extension user will hear a "beep" tone when there is a call waiting in the extension's queue.
Play the Newest Voice Message First	Selected, new voicemail will be retrieved first. When not selected, the system will play voicemail based on first-in-first-out (FIFO).

Press Zero Option

This option allows a caller to press "0" while listening to this extension's greeting. Use the drop-down list to select one of the following forwarding destinations for the call: **Voice Mail**, **AA**, **Extension**, **Group**, **Operator** (default), **Outside Number**, **Application Extension**, or **Line Park**. When the caller presses "0", the call will forward to the specified destination.

Setting Mailbox Capacities

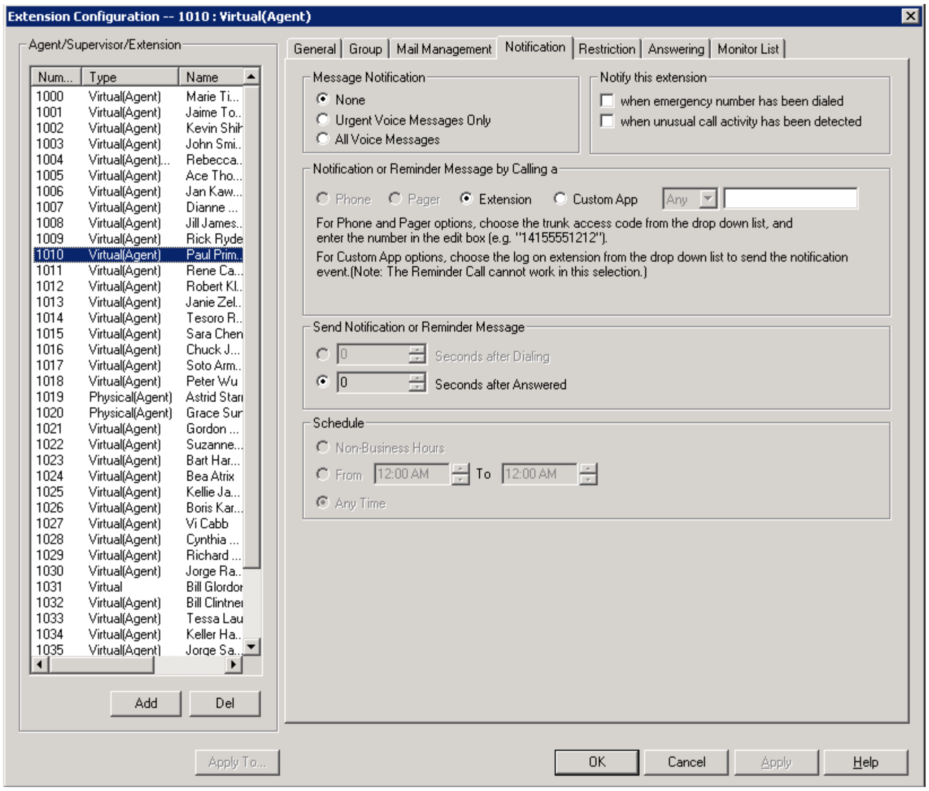
You can set various mailbox capacities with the following options:

Parameter	Description
Max Number of Messages	Maximum number of messages stored in the user's mailbox. The range is **1**–**999**, defaulting to 100.
Mailbox Size	Mailbox size in MBs of stored messages. The range is **1**–**500** MB, with a default of 50.
Max Message Length	Maximum length of voice messages in minutes. The range is **1**–**30** minutes, with a default of 5 minutes.
Retention Length of Saved Messages	Number of days saved messages are archived by the system. The range is **1**–**90** days, with a default of 60.

These options can be applied to multiple extensions using **Apply to**.

Setting Message Notification Options

The **Notification** tab of Extension Configuration provides for setting notification options on new incoming e-mail as well as voice messages. To work with notification settings, select the extension number from the **Agent/Supervisor/Extension** list, then click the **Notification** tab.



Extension Configuration -- 1010 : Virtual(Agent)

Agent/Supervisor/Extension

Num...	Type	Name
1000	Virtual(Agent)	Marie Ti...
1001	Virtual(Agent)	Jaime To..
1002	Virtual(Agent)	Kevin Shih
1003	Virtual(Agent)	John Smi..
1004	Virtual(Agent)...	Rebecca..
1005	Virtual(Agent)	Ace Tho...
1006	Virtual(Agent)	Jan Kaw...
1007	Virtual(Agent)	Dianne ...
1008	Virtual(Agent)	Jill James..
1009	Virtual(Agent)	Rick Ryde
1010	Virtual(Agent)	Paul Prim..
1011	Virtual(Agent)	Rene Ca...
1012	Virtual(Agent)	Robert Kl..
1013	Virtual(Agent)	Janie Zel..
1014	Virtual(Agent)	Tesoro R..
1015	Virtual(Agent)	Sara Chen
1016	Virtual(Agent)	Chuck J...
1017	Virtual(Agent)	Soto Arm..
1018	Virtual(Agent)	Peter Wu
1019	Physical(Agent)	Astrid Star
1020	Physical(Agent)	Grace Sur
1021	Virtual(Agent)	Gordon ...
1022	Virtual(Agent)	Suzanne...
1023	Virtual(Agent)	Bart Har...
1024	Virtual(Agent)	Bea Atrix
1025	Virtual(Agent)	Kellie Ja...
1026	Virtual(Agent)	Boris Kar...
1027	Virtual(Agent)	Vi Cabb
1028	Virtual(Agent)	Cynthia ...
1029	Virtual(Agent)	Richard ...
1030	Virtual(Agent)	Jorge Ra..
1031	Virtual	Bill Glordor
1032	Virtual(Agent)	Bill Clintner
1033	Virtual(Agent)	Tessa Lau
1034	Virtual(Agent)	Keller Ha..
1035	Virtual(Agent)	Jorge Sa...

Message Notification
● None
○ Urgent Voice Messages Only
○ All Voice Messages

Notify this extension
□ when emergency number has been dialed
□ when unusual call activity has been detected

Notification or Reminder Message by Calling a
○ Phone ○ Pager ● Extension ○ Custom App Any

For Phone and Pager options, choose the trunk access code from the drop down list, and enter the number in the edit box (e.g. "14155551212").

For Custom App options, choose the log on extension from the drop down list to send the notification event.(Note: The Reminder Call cannot work in this selection.)

Send Notification or Reminder Message
○ 0 Seconds after Dialing
● 0 Seconds after Answered

Schedule
○ Non-Business Hours
○ From 12:00 AM To 12:00 AM
● Any Time

Figure 15-8. Extension Configuration, Notification tab

Individual users can also configure **Message Notification** within the MaxAgent for Lync.

Note: You can use **Apply to** to apply notification settings to one, some, or all extensions. See "Using the Apply To Button" on page 124 for more information on using **Apply to**.

Setting the Message Types for Notification

Select the types of messages for which the extension user is notified:

- **None**—No notification. Selecting this option does not prevent the user from getting message waiting indicators or stutter dial tone when new messages are received.
- **Urgent Voice Messages Only**
- **All Voice Messages**

The system will perform notification under the following conditions:

- Extension's message notification is set to **Urgent Voice Messages Only**.
- Extension's notification Schedule is set to **Non-Business Hours**.
- Voice mail received during business hours is marked urgent.
- Extension user does not check the urgent message.

The system will start notification as soon as it enters non-business hours.

Note: Message notification can also be set in MaxAgent, and the settings are reflected in MaxACD Administrator.

Emergency Notification

When any extension dials an emergency number, the system can make calls to specified extensions, groups, or outside numbers. To configure this option, select the extension/group/outside number, and check the **When Emergency Number Has Been Dialed** check box.

Emergency-number calls are logged to *SecurityAlert.txt* (see "Where Security Alerts Are Logged" on page 135.)

Unusual VM Activity Notification

When certain unusual activity is detected from an extension's voice mail, the system can notify a designated extension. This option is intended to help detect if a hacker has obtained control of and is making calls from an extension's voice mail. To alert an extension (usually the administrator) when either of the following abnormal activities are happening, select the extension and check the option **When unusual call activity has been detected**:

- When calls made from voice mail are unusually long (by default, more than 120 minutes)
- When the number of calls made from voice mail is unusually high (by default, more than 20 calls in one voice mail session)

When the designated extension is notified, the system will play "Unusual call activity has been detected from Extension xxxx. More than yy calls have been made from the extension's voice mail. Please verify with the extension user." Or "Unusual call activity has been detected from Extension xxxx. The extension made more than a yyy-minute call from the extension's voice mail. Please verify with the extension user." The security notification will be made only once within a call.

Setting Parameters for Unusual VM Activity

To change the parameters for the number of calls or length of a call, you must add the following strings and values to the Windows registry:

- *SecurityConnectionDuration* (value range is from 1-1440 minutes [24 hours]). When the setting is out of range, the default of 120 minutes will be used.
- *SecurityNumberOfCalls* (value range is from 1-100 calls). When the setting is out of range, the default of 20 calls will be used.

Adding security values to the registry

To add one or both of the above security values to the Windows registry:

1. Choose **Run** from the Windows **Start** menu, type **regedit**, and click **OK**.
2. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\AltiGen Communications, Inc.\AltiWare\InitInfo**.
3. On the right side of the Registry window, right-click and choose **New > DWORD Value**.
4. Type one of the security strings listed above, then double-click the entry.
5. Choose **Decimal** as the **Base** option.
6. Type the value you want (see the allowed range listed above) in the **Value data** text box, and click **OK**.
7. The value you enter appears in parentheses in the **Data** column.

8. For the values you entered in the registry to take effect, from the MaxACD Administrator menu, choose **Diagnostic > Trace**. The Trace Filter dialog box opens. Click the **Minute Task** button in the dialog box. Alternatively, you could restart the system for the values to take effect.

   Note: To have access to the commands on the **Diagnostic** menu, you must first log into MaxACD Administrator with the password *jazzy* and then again with the administrator password.

Where Security Alerts Are Logged

Security alerts are logged to **...\AltiServ\Log\SecurityAlert.txt**. The log includes date, time, extension number, pad number, and the alert reason. Emergency calls are also logged to this file. Following are some examples:

```
2010-02-04 08:30:25 Extension 212 made more than 20 calls from voicemail(1:2)
2010-02-04 16:00:50 Extension 395 made more than a 120-minute call from voicemail(0:6).
2010-02-18 09:05:32 Extension 395(2:3) made an emergency call-###.
```

Note: A *SecurityAlert.txt* file does not appear in the **...AltiServ\Log** folder until a security alert event has created it.

Setting the Type of Notification

There are four options for sending the notification or reminder message: **phone**, **pager**, **extension** or **custom application (Custom App)**.

- **Phone/Pager**—for the **Phone** and **Pager** options, first specify the trunk or route access code using the drop-down list. The **Any** option means to locate any available trunk. Then type in the number with all relevant dialing prefixes other than the trunk code, using a maximum of 63 digits.
- **Extension**—to use the Extension option, select the **Extension** radio button, then type the extension number into the text box.
- **Custom App**—when used in conjunction with a third-party notification application, the **Custom App** feature enables an extension to connect to an application that can receive the notification event; use the drop-down list to choose the log-on extension to which the third-party application is connected. Contact your local AltiGen dealer for more information on using this feature.

  Note: The Reminder Call will not work with this selection.

Note also the following considerations:

- For the **Pager** option, the system calls the specified pager number and then dials the system main number (as set in System Configuration, **General** tab), which is then displayed on the user's pager.

  For the operator-assisted paging function, the operator phone number **and** the pager number must be entered in the **<phone number>*<pager number>** format. For example, if the phone number to call the pager operator is **7654321** and the pager number to page the user is **12345678**, the notification outcall number that needs to be entered is **7654321*12345678**. When the pager operator answers the Message Notification call, MaxACD announces the **pager number and** the **System Main Number** (as configured on the **General** tab of **System Configuration**), which will be displayed on the user's pager. The operator is also given the option to repeat these numbers by pressing '**#**'.

Outcall to Cellular or PCS Phone Numbers

When an outcall is made by the system (for Message Notification, Call Forwarding, and so on) to a cellular or PCS phone, it may ring the phone once but not necessarily present the call and make a connection. This will happen if the ringback tone played by the cellular service provider does not conform to standard ringback tones. To work around this problem, append a few commas (**,**) to the outcall (cellular) number when entering it. Each comma provides a one second pause.

Setting Notification Timing

When notification is configured to an *outside phone number*, the system will announce, "This is the outcall notification message for…" after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the carrier. If the system plays the announcement phrase before the notification call is answered, the phrase will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing—**If the carrier of the outside phone number cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)

  Note: Note: If the delay is set too long, the notified party will hear silence before the announcement is played.

- **Seconds after Answered—**This field is set to 0 seconds and it is not configurable for notification to a phone number. It means the system will play the announcement immediately after answer supervision is received.

When notification is configured to a *pager*, the system will transmit DTMF digits as the return phone number (the **System Main Number** as set in the System Configuration **General** tab) after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the pager system. If the system sends digits before the call is connected, some digits will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing—**If the pager carrier cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)
- **Seconds after Answered—**If the answer supervision signal is provided by the carrier, check this option and set the delay timer to 2 to 5 seconds. In some cases, the pager carrier cannot detect DTMF right after the call connection. (Default is 10 seconds, maximum is 30.)

  Note: You may need to try a different delay setting to make sure the user return number is transmitted properly after configuration.

Setting Notification Business Hours

You can choose one of three options for when the extension user is to be notified of new messages:

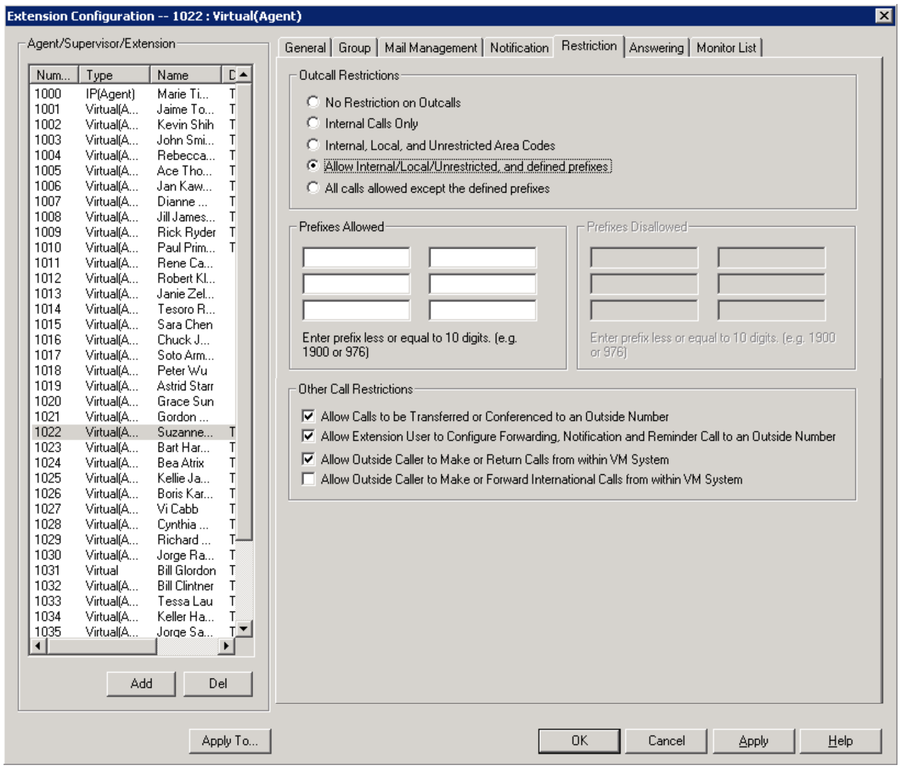
- **Non-Business Hours**—notification only during non-business hours. Business hours are set in System Configuration, **Business Hours** tab (see "Setting Business Hours" on page 39).
- **From/To**—notification during a specified time of day. Select the hours in the **From** and **To** time scroll boxes.
- **Any Time**—notification at all times (every day).

Enabling Message Notification

After configuring your message notification settings, to enable message notification, check the **Allow Extension User to Configure Forwarding, Notification and Reminder Call to an Outside Number** check box on the **Restriction** tab of Extension Configuration.

Configuring Calling Restrictions

To work with extension call restrictions, select the extension number you want to work with from the **Agent/Supervisor/Extension** list, then click the **Restriction** tab.



Extension Configuration -- 1022 : Virtual(Agent)

Agent/Supervisor/Extension

Num...	Type	Name	D
1000	IP(Agent)	Marie Ti...	T
1001	Virtual(A...	Jaime To...	T
1002	Virtual(A...	Kevin Shih	T
1003	Virtual(A...	John Smi...	T
1004	Virtual(A...	Rebecca...	T
1005	Virtual(A...	Ace Tho...	T
1006	Virtual(A...	Jan Kaw...	T
1007	Virtual(A...	Dianne ...	T
1008	Virtual(A...	Jill James...	T
1009	Virtual(A...	Rick Ryder	T
1010	Virtual(A...	Paul Prim...	T
1011	Virtual(A...	Rene Ca...	
1012	Virtual(A...	Robert Kl...	
1013	Virtual(A...	Janie Zel...	
1014	Virtual(A...	Tesoro R...	
1015	Virtual(A...	Sara Chen	
1016	Virtual(A...	Chuck J...	
1017	Virtual(A...	Soto Arm...	
1018	Virtual(A...	Peter Wu	
1019	Virtual(A...	Astrid Starr	
1020	Virtual(A...	Grace Sun	
1021	Virtual(A...	Gordon ...	
1022	Virtual(A...	Suzanne...	T
1023	Virtual(A...	Bart Har...	T
1024	Virtual(A...	Bea Atrix	T
1025	Virtual(A...	Kellie Ja...	T
1026	Virtual(A...	Boris Kar...	T
1027	Virtual(A...	Vi Cabb	T
1028	Virtual(A...	Cynthia ...	T
1029	Virtual(A...	Richard ...	T
1030	Virtual(A...	Jorge Ra...	T
1031	Virtual	Bill Glordon	T
1032	Virtual(A...	Bill Clintner	T
1033	Virtual(A...	Tessa Lau	T
1034	Virtual(A...	Keller Ha...	T
1035	Virtual(A...	Jorge Sa...	T

Outcall Restrictions

○ No Restriction on Outcalls
○ Internal Calls Only
○ Internal, Local, and Unrestricted Area Codes
● Allow Internal/Local/Unrestricted, and defined prefixes
○ All calls allowed except the defined prefixes

Prefixes Allowed

Enter prefix less or equal to 10 digits. (e.g. 1900 or 976)

Prefixes Disallowed

Enter prefix less or equal to 10 digits. (e.g. 1900 or 976)

Other Call Restrictions

☑ Allow Calls to be Transferred or Conferenced to an Outside Number
☑ Allow Extension User to Configure Forwarding, Notification and Reminder Call to an Outside Number
☑ Allow Outside Caller to Make or Return Calls from within VM System
☐ Allow Outside Caller to Make or Forward International Calls from within VM System

Figure 15-9. Extension Configuration, Restriction tab

Note: You can use **Apply to** to apply call restriction settings to one, some, or all extensions. See “Using the Apply To Button” on page 124 for more information on using **Apply to**.

Setting Call Restriction Options

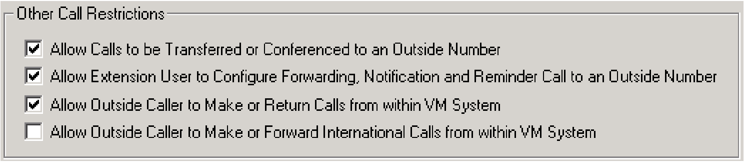
You can use one of the following options in setting restrictions on an extension or on multiple extensions using **Apply to**.

- **No Restrictions on Outcalls**
- **Internal Calls Only**—extension-to-extension.

- **Internal, Local, and Unrestricted Area Codes**—Allow extension to call internal, local, and area codes defined in the **Unrestricted Area Codes** in the **Call Restriction** tab of the System Configuration window.
- **Allow Internal/Local/Unrestricted, and Defined Prefixes**—In addition to the above privilege, allow the extension to call prefixes you specify in the **Prefixes Allowed** boxes. Include all relevant prefix numbers (for example, if appropriate, you would include 1+area code before the number). This configuration will not override **System Prohibited Prefixes** set in System Configuration.
- **All Calls Allowed Except the Defined Prefixes**—In addition to System Prohibited Prefixes, you can block this extension from dialing the numbers defined in the **Prefixes Disallowed** boxes.

Setting Other Call Restrictions

Other call restriction rules can deny or allow the following:



Other Call Restrictions

☑ Allow Calls to be Transferred or Conferenced to an Outside Number
☑ Allow Extension User to Configure Forwarding, Notification and Reminder Call to an Outside Number
☑ Allow Outside Caller to Make or Return Calls from within VM System
□ Allow Outside Caller to Make or Forward International Calls from within VM System

Figure 15-10. Call Restriction Rules

- **Allow Calls to be Transferred or Conferenced to an Outside Number**—when checked, the internal extension user can log into voice mail, make a call to a second party, then transfer or conference to a third party.
- **Allow User to Configure Forwarding, Notification, and Reminder Call to an Outside Number**—This setting regulates extension call forwarding, voice mail notification, and reminder call configuration. If this setting is not checked, you will see a warning message pop up when trying to set up forwarding to an outside number. International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Return Calls from within VM System**—when checked, an outside caller can dial into the system, log in to the extension’s voice mail, and make or return calls from the voice mail (Zoomerang feature). International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Forward International Calls from within VM system**—This setting regulates making international calls from voice mail and forwarding to an international number. You need to check the second and third options to be able to check this configuration.

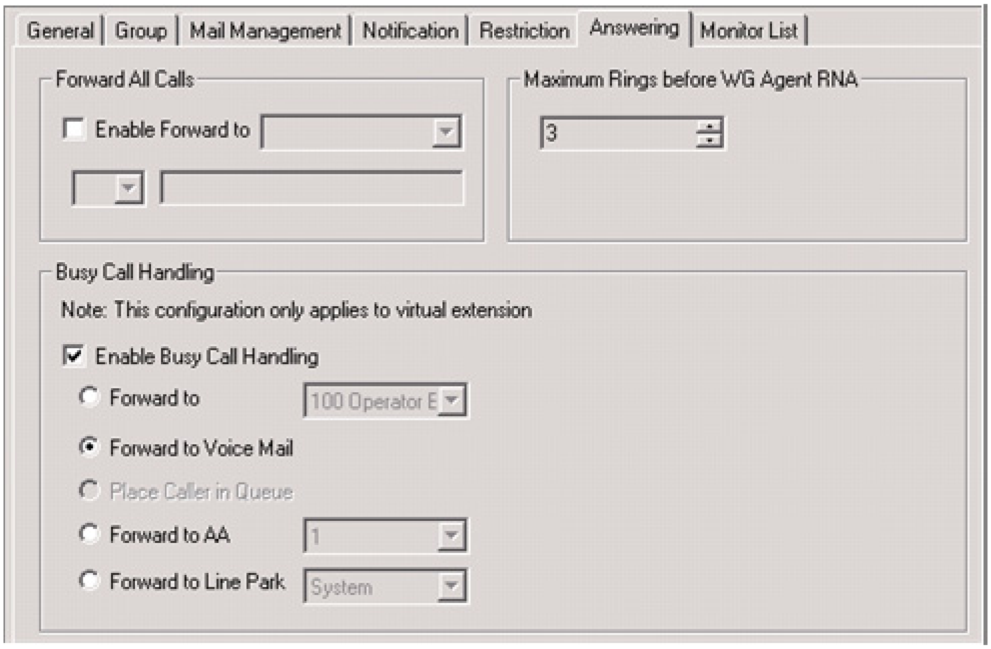
Caution! Allowing any of these options may increase the potential for toll fraud. Make sure the password is properly configured to prevent an intruder from using this voice mail box to make an outbound call. AltiGen recommends that you leave the fourth option unchecked for all extensions at all times.

Setting Answering Options

Answering options include forwarding, handling busy calls, handling no-answers and other options.

You can use the **Apply to** button to apply answering settings to one, some, or all extensions. See "Using the Apply To Button" on page 124 for more information.

To work with extension answering options, select the extension number from the **Agent/Supervisor/Extension** list, then click the **Answering** tab.



Forward All Calls

☐ Enable Forward to

Maximum Rings before WG Agent RNA: 3

Busy Call Handling

Note: This configuration only applies to virtual extension

☑ Enable Busy Call Handling

○ Forward to: 100 Operator E

● Forward to Voice Mail

○ Place Caller in Queue

○ Forward to AA: 1

○ Forward to Line Park: System

Figure 15-11. Extension Configuration, Answering tab

- **Maximum Rings before WG Agent RNA** – This indicates, for the current agent, how many rings to allow before the system follows the workgroup agent "Ring No Answer" rules.

Forwarding All Calls

These types of call forwarding are available:

A One Hop Limit to Call Forwarding for a Transferred Call

There is a one hop limit to call forwarding when the call that is being passed is a transferred call. For example, extension 100 receives a transferred call and forwards this call to extension 101; extension 101 is set to forward all calls to extension 102; extension 102 receives the call but CANNOT forward this call to another extension.

A 10-Hop Limit to Call Forwarding for Direct Calls

For direct calls, there is a "10-hop" limit to call forwarding. For example, extension 100 forwards to extension 101, 101 forwards to 102, 102 forwards to 103, and so on, through extension 120. A call to extension 100 will be forwarded to 101, which will forward to 102, which will forward to 103, and so on, until the call has been forwarded 10 times. At this point, the call will not be forwarded again; if the last extension in the forwarding chain does not answer, the call is sent to extension 100's voice mail.

If there is a loop condition in the forwarding chain (for example, 100 forwards to 101, 101 to 102, and 102 back to 100), the call is sent to the first destination's voice mail.

To enable call forwarding, check the **Enable Call Forward to** check box, then, using the drop-down list, indicate the forwarding destination. You can use **Apply to** to act on multiple extensions, with the restrictions discussed in the previous section. The forwarding options are as follows:

- To **Voice Mail**
- To **AA**—select the auto attendant number to use in the drop-down list under the option.
- To an **Extension**—select an extension from the drop-down list.
- To a **Group**—select a group from the drop-down list.
- To the **Operator**
- To an **Outside Number**—this option is available if it is allowed in the **Other Call Restrictions** option in the **Restriction** tab, as discussed in "Setting Other Call Restrictions" on page 138. Also, see "Outcall to Cellular or PCS Phone Numbers" on page 136.

  If you choose **Outside Number**, select a trunk or route access code to use in the small drop-down list on the left, and type in the full prefix and phone number.
- To an **App Ext**—when used in conjunction with an SDK-based application.
- To **Line Park**—if configured, select a **Line Park** group (configured in "Line Park Configuration" on page 147) from the drop-down list.
- To **Free Format**

  You can enter up to 40 digits and can use 0-9, *, #, and ",". One "," represents one second of delay.

  You can use this configuration to send out additional DTMF digits to an extension, workgroup, or outside number. Here is an example: Extension 100 is set to forward all calls to "200,,,123". Extension 101 makes a call to extension 100. The call is forwarded to 200. If 200 is an extension, 3 seconds after extension 200 picks up the call, extension 200 should hear DTMF tones (123). If 200 is a workgroup with agent 201 and 202, when the agent (either 201 or 202) picks up the call, after 3 seconds the agent should hear DTMF tones (123).

  Two other examples using **Free Format**: "92529712,,,,,5,,,211" means dial trunk access code 9, and an outside number 2529712, wait 5 seconds, dial 5, and wait 3 seconds, then dial 211. Second example: "102,,01,,,5#" means dial extension 102, wait 2 seconds, dial 01, wait 3 seconds, and then dial 5#.

  For a trunk call, the wait time starts right after the digits are dialed (even while the target phone is ringing). For an extension call, the wait time starts after connecting to the extension (it does not start when ringing begins).
- To **Paging Trunk**—To use this option, you have to select a paging trunk in Trunk Configuration.
- To **VM Access**—To access the AltiGen mailbox for the extension selected from the drop-down list.

Note: Forwarding calls to a pager is possible but **not recommended** since callers will only hear what is heard when calling a pager and will not know to enter a return phone number unless instructed.

Handling Busy Calls

You have several options for handling calls while the extension is busy. If you do not enable busy call handling, the caller simply hears a busy signal.

To enable the options, check the **Enable Busy Call Handling** check box, then select from the following options:

- **Forward to Extension**—Select an extension number in the drop-down list. See "A 10-Hop Limit to Call Forwarding for Direct Calls" on page 139.
- **Forward to Voice Mail**
- **Forward to AA**—select the auto attendant number to use in the drop-down list under the option.
- **Forward to Line Park**—use the drop-down list to select a Line Park group to route the call to. (See "Line Park Configuration" on page 147.)

Setting Up Monitor Lists

The **Monitor List** tab provides for setting up lists of extensions for which call processing events can be monitored by the extension user. Once a monitor list is established, the application logging into the extension can receive call events for the monitored extensions. The monitor list is available in the MaxAgent **Monitor** tab and in Line Monitoring events in AltiGen SDK.

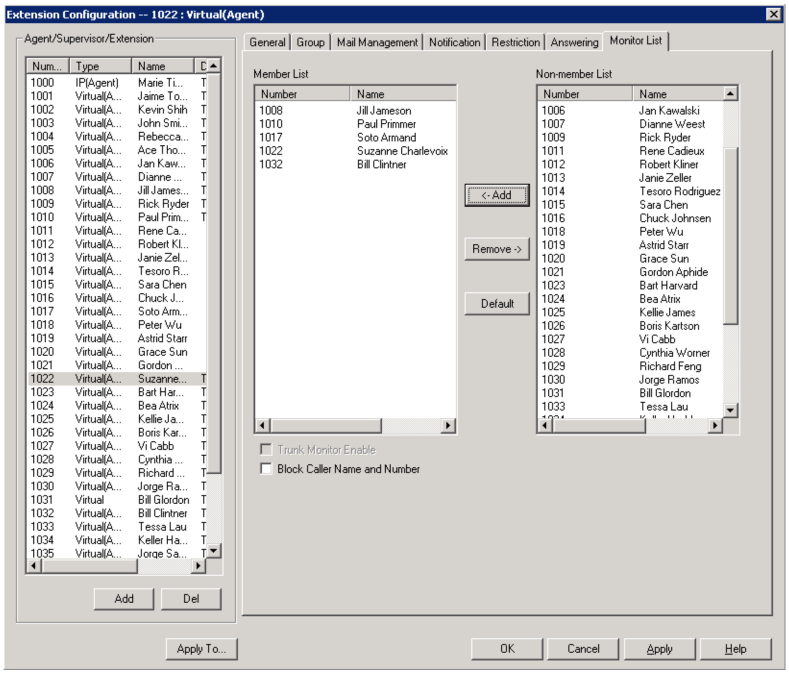
WARNING! Listening in to or recording a conversation without the consent of one or both parties may be a violation of local, state, and federal privacy laws. It is the responsibility of the users of this feature to assure they are in compliance with all applicable laws.

Restrictions and Defaults

- If you place an extension in a Monitor List, that extension will show in the user's MaxAgent **Monitor** tab.
- In MaxSupervisor, the user can monitor only the workgroup(s) he or she logs in to, regardless of the monitoring rights assigned to his or her extension in MaxACD Administrator.

Configuring a Monitor List

To set up a monitor list, select the extension number to receive the monitoring rights from the **Agent/Supervisor/Extension** list, then click the **Monitor List** tab.



Num...	Type	Name	C
1000	IP(Agent)	Marie Ti...	T
1001	Virtual(A...	Jaime To...	T
1002	Virtual(A...	Kevin Shih	T
1003	Virtual(A...	John Smi...	T
1004	Virtual(A...	Rebecca...	T
1005	Virtual(A...	Ace Tho...	T
1006	Virtual(A...	Jan Kaw...	T
1007	Virtual(A...	Dianne ...	T
1008	Virtual(A...	Jill James...	T
1009	Virtual(A...	Rick Ryder	T
1010	Virtual(A...	Paul Prim...	T
1011	Virtual(A...	Rene Ca...	
1012	Virtual(A...	Robert Kl...	
1013	Virtual(A...	Janie Zel...	
1014	Virtual(A...	Tesoro R...	
1015	Virtual(A...	Sara Chen	
1016	Virtual(A...	Chuck J...	
1017	Virtual(A...	Soto Arm...	
1018	Virtual(A...	Peter Wu	
1019	Virtual(A...	Astrid Starr	
1020	Virtual(A...	Grace Sun	
1021	Virtual(A...	Gordon ...	
1022	Virtual(A...	Suzanne...	T
1023	Virtual(A...	Bart Har...	T
1024	Virtual(A...	Bea Atrix	T
1025	Virtual(A...	Kellie Ja...	T
1026	Virtual(A...	Boris Kar...	T
1027	Virtual(A...	Vi Cabb	T
1028	Virtual(A...	Cynthia ...	T
1029	Virtual(A...	Richard ...	T
1030	Virtual(A...	Jorge Ra...	T
1031	Virtual	Bill Glordon	T
1032	Virtual(A...	Bill Clintner	T
1033	Virtual(A...	Tessa Lau	T
1034	Virtual(A...	Keller Ha...	T
1035	Virtual(A...	Jorge Sa...	T

Member List

Number	Name
1008	Jill Jameson
1010	Paul Primmer
1017	Soto Armand
1022	Suzanne Charlevoix
1032	Bill Clintner

Non-member List

Number	Name
1006	Jan Kawalski
1007	Dianne Weest
1009	Rick Ryder
1011	Rene Cadieux
1012	Robert Kliner
1013	Janie Zeller
1014	Tesoro Rodriguez
1015	Sara Chen
1016	Chuck Johnsen
1018	Peter Wu
1019	Astrid Starr
1020	Grace Sun
1021	Gordon Aphide
1023	Bart Harvard
1024	Bea Atrix
1025	Kellie James
1026	Boris Kartson
1027	Vi Cabb
1028	Cynthia Worner
1029	Richard Feng
1030	Jorge Ramos
1031	Bill Glordon
1033	Tessa Lau

☐ Trunk Monitor Enable
☐ Block Caller Name and Number

Figure 15-12. Extension Configuration, Monitor List tab

To add members to the list

1. From the **Monitor Available** list, select the extensions the user will have a right to monitor.
2. Click **Add** to move the extensions to the **Monitor List**.

To remove members

1. Select the extensions in the **Monitor List.**
2. Click **Remove.**

Other Options	Description
Default button	Returns to the default - the extension can monitor its own calls only.
Trunk Monitor Enable	Allows monitoring of the AltiGen SDK trunk events at the selected extension.
Block Caller Name and Number	When a monitored extension receives a call, blocks the display of the caller’s name and number in the monitor tab of the client application.

CHAPTER

16

Routing Unassigned Extensions

You can configure MaxACD to route a call to an unassigned extension to

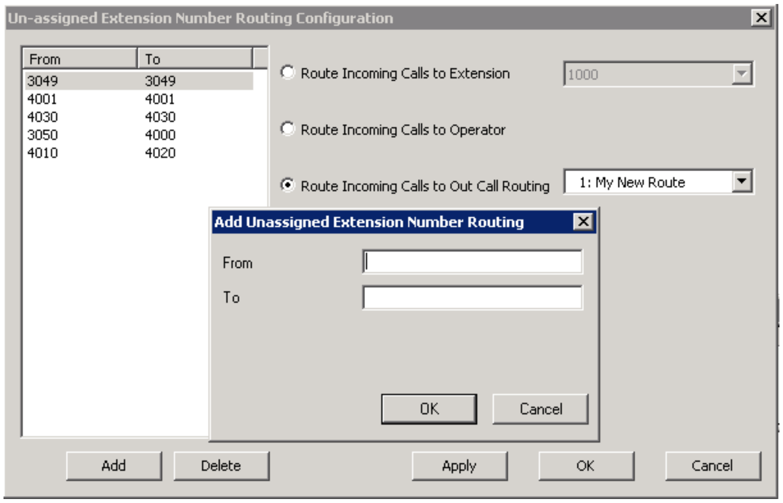
- Another extension
- The operator
- An external number (which must be a route definition you've created in **General > Out Call Routing Configuration**).

If you don't configure this, callers will hear an "invalid number" message when they dial an unassigned extension.

You can configure the routes of calls to single extension numbers and to ranges of numbers.

Configuring the Route

1. Select **General > Unassigned Extension Number Configuration** and click **Add**.



Un-assigned Extension Number Routing Configuration

From	To
3049	3049
4001	4001
4030	4030
3050	4000
4010	4020

○ Route Incoming Calls to Extension 1000

○ Route Incoming Calls to Operator

● Route Incoming Calls to Out Call Routing 1: My New Route

Add Unassigned Extension Number Routing

From

To

Figure 16-1. Unassigned Extenstion Routing dialog box

2. Enter the range of the unassigned extension(s) you want to route:

In the **From** field. enter the first extension of the range. Make sure it has the same number of digits as defined in **System Configuration > Number Plan** tab **> Number Length** field. The extension you enter appears in the **To** field also. If you’re specifying a single extension, click **OK**. If you’re specifying a range of extensions, enter the end of the range in the **To** field, and then click **OK**.

- Only digits are allowed
- Ranges can be nested, but overlapping ranges are not allowed.
- When the ranges are nested, the smaller range takes priority: the route configured for the smaller range is the one used.
- If there are assigned extensions within the specified range, calls to those extensions will still go to the assigned extension. Only calls to *un*assigned extensions will follow the routing you specify here. For example, if the range is between 2095 and 3000, and there's an assigned extension 2098, then the only extension numbers that get rerouted are are 2095, 2096, 2097, 2099, and 3000.

Example:

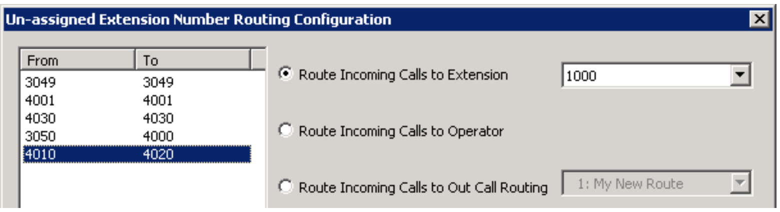
Assume an unassigned extension routing entry already exists: 1000-1600.

Range 1600-1700 cannot be added, because it overlaps with 1000-1600.

Range 1601-1700 can be added, because it is independent from 1000-1600.

Range 1500-1600 can be added, because it is contained by (nested within) 1000-1600.

3. Select the new range and then select where to route the call:



Un-assigned Extension Number Routing Configuration

From	To
3049	3049
4001	4001
4030	4030
3050	4000
4010	4020

● Route Incoming Calls to Extension: 1000

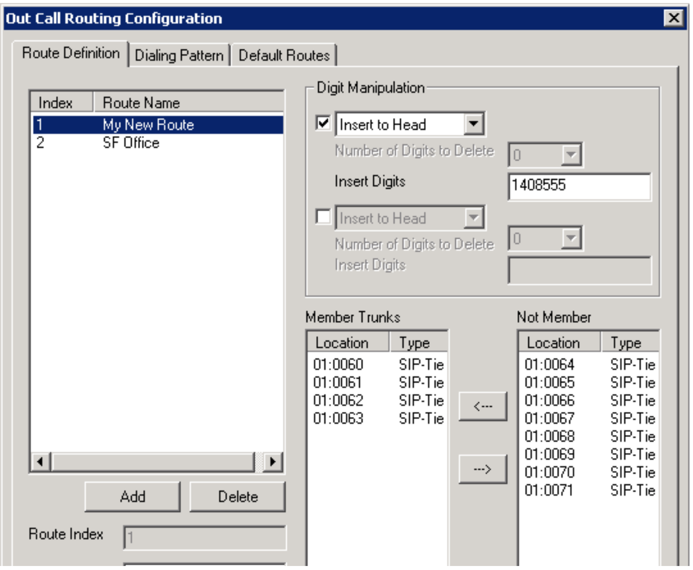
○ Route Incoming Calls to Operator

○ Route Incoming Calls to Out Call Routing: 1: My New Route

Figure 16-2.   Unassigned Extention Routing range

If you’re routing to an extension, select an extension from the drop-down list.

To route calls to out call routing, you must have configured route definitions in **General > Out Call Routing**:



Index	Route Name
1	My New Route
2	SF Office

Route Index: 1

Digit Manipulation

☑ Insert to Head
Number of Digits to Delete: 0
Insert Digits: 1408555

□ Insert to Head
Number of Digits to Delete: 0
Insert Digits:

Member Trunks

Location	Type
01:0060	SIP-Tie
01:0061	SIP-Tie
01:0062	SIP-Tie
01:0063	SIP-Tie

Not Member

Location	Type
01:0064	SIP-Tie
01:0065	SIP-Tie
01:0066	SIP-Tie
01:0067	SIP-Tie
01:0068	SIP-Tie
01:0069	SIP-Tie
01:0070	SIP-Tie
01:0071	SIP-Tie

Figure 16-3.   Out Call Routing dialog box

Routing Unassigned Extensions to Lync Server

To route unassigned extensions to the Lync server,

1. In Enterprise Manager, determine the Lync Server location ID. You will enter this ID number in the next step.
2. In MaxACD Admin, create an out call routing definition. (For details on creating this definition, see “Working with Route Definitions” on page 116.) You will use this definition name in step 4.
   - Add SIP-Tie trunks to Member Trunks.
   - Select **Insert to Header** and enter the Lync Server location ID (from step 1) into the *Insert Digits* field.
3. Select **General > Unassigned Extension Number Configuration** and click **Add**.
4. Add the range of extensions. Choose that range, select “Route Incoming Calls to Out Call Routing” and pick the route name you created in step 2.
5. In the Lync Server control panel, click Users. Make sure the regular Lync users have the correct extension formatting for *Line URI*. Use either of these two acceptable formats (substitute correct numbers for the example numbers shown):
   - `Tel:+14085551212;ext=504`
   - `Tel:504`

Deleting a Route

To delete a route, select it and click the **Delete** button.

CHAPTER 17

Line Park Configuration

The Line Park feature is a kind of call park method. Line Park IDs can be grouped as a Line Park Group for call routing purposes; the system call park ID is assigned by the system automatically.

The Line Park feature can be used for the following applications:

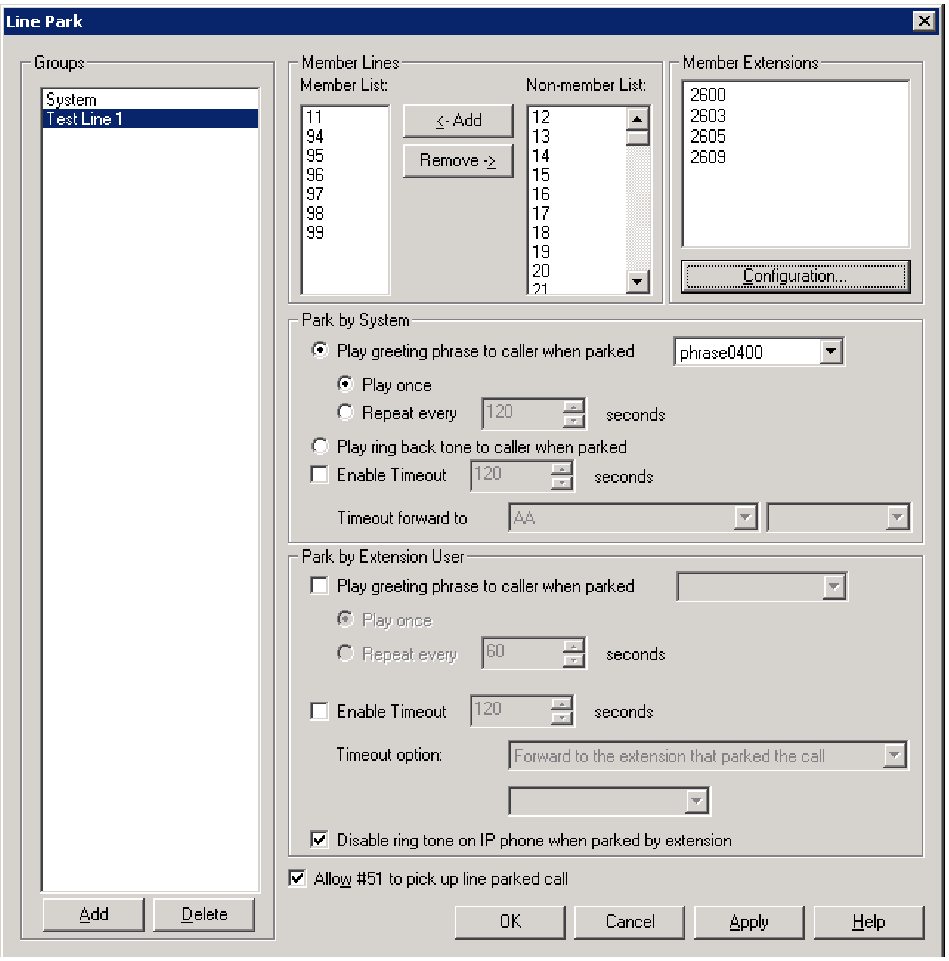
- Inbound call line appearance during business hours
- Operator parks a call for a group of IP phone users
- Executive/assistance call coverage
- Night hours call coverage
- Overflow new workgroup calls to a Line Park Group when the queue length or queue time is too long.

Implementation notes

- A total of 99 (01 to 99) line IDs can be grouped into different Line Park Groups. The default "System" group cannot be removed.
- One Line Park ID can belong to only one group.
- A Line Park Group can be assigned to:
    - Trunk In-Call Routing
    - Extension/Workgroup Busy or RNA Handling
    - Extension/Workgroup Forwarding
    - Workgroup Quit Queue Option
- Extensions can be assigned as members of Line Park Groups, allowing the extension users to see and pick up a parked call from those groups in the **LinePark** tab of their MaxAgent.
- The system will put the caller in queue when calls exceed the total lines assigned to the Line Park Group.
- The parked line is released when the call disconnects, is answered, or is forwarded due to time out.

Line Park Configuration

To configure line park, select **General > Line Park Configuration**.



Groups: System, Test Line 1

Member Lines

Member List: 11, 94, 95, 96, 97, 98, 99

Non-member List: 12, 13, 14, 15, 16, 17, 18, 19, 20, 21

Member Extensions: 2600, 2603, 2605, 2609

Park by System

● Play greeting phrase to caller when parked: phrase0400

● Play once

○ Repeat every 120 seconds

○ Play ring back tone to caller when parked

□ Enable Timeout 120 seconds

Timeout forward to: AA

Park by Extension User

□ Play greeting phrase to caller when parked

● Play once

○ Repeat every 60 seconds

□ Enable Timeout 120 seconds

Timeout option: Forward to the extension that parked the call

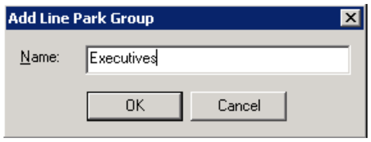
☑ Disable ring tone on IP phone when parked by extension

☑ Allow #51 to pick up line parked call

Figure 17-1. Line Park Configuration window

Setting Up a Line Park Group

1. In the **Line Park Configuration** window, click the **Add** button below the **Groups** list.

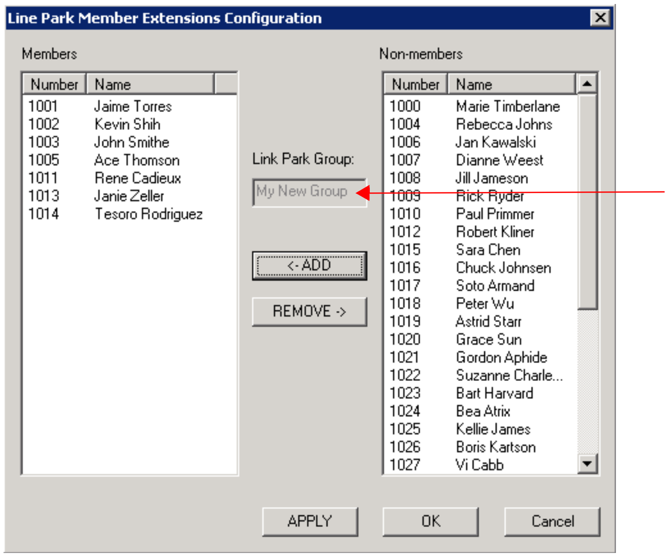


Name: Executives

Figure 17-2. Add Line Park dialog box

2. Enter a name in the **Add Line Park** dialog box, and click **OK**.

3. Select line ID numbers from the **Non-Member List** and click the **Add** button to add them to the **Member List**.
4. To assign extensions to a group, select the group, and then click the **Configuration** button below the Member Extensions panel.



Members

Number	Name
1001	Jaime Torres
1002	Kevin Shih
1003	John Smithe
1005	Ace Thomson
1011	Rene Cadieux
1013	Janie Zeller
1014	Tesoro Rodriguez

Link Park Group: My New Group

Non-members

Number	Name
1000	Marie Timberlane
1004	Rebecca Johns
1006	Jan Kawalski
1007	Dianne Weest
1008	Jill Jameson
1009	Rick Ryder
1010	Paul Primmer
1012	Robert Kliner
1015	Sara Chen
1016	Chuck Johnsen
1017	Soto Armand
1018	Peter Wu
1019	Astrid Starr
1020	Grace Sun
1021	Gordon Aphide
1022	Suzanne Charle...
1023	Bart Harvard
1024	Bea Atrix
1025	Kellie James
1026	Boris Kartson
1027	Vi Cabb

The name of the selected group appears here

Figure 17-3. Configuring a Line Park group's member extensions

5. Select members for this Line Park group from the Non-Members list, and click the **Add** button to move them to the Members list.

   Members of a Line Park group can use their MaxAgent applications to see and pick up calls parked for this group.

   Any extension can park a call to any group. Any extension can pick up a call from any group using #51 followed by the line park location, if allowed by MaxACD Administrator configuration.
6. Configure the following **Line Park** options:

   Park by System:

   - **Play greeting phrase to caller when parked**—Select this option to have the system play the greeting phrase you select from the drop-down box, before playing music on hold. Specify whether to play the greeting once only, or every x seconds.
   - **Play ring back tone to caller when parked**—Select this option when you want the caller to hear a ring back tone if the call has not been answered by any extension or voice mail. If the call is answered and parked, the caller will hear a greeting phrase and on-hold music.
   - **Enable Timeout**—When you check this box, a line park call will time out after the number of seconds set in the value box. Use the **Timeout forward to** drop-down boxes to route the call to an AA, voice mail, or an extension/group.

   Park by Extension User:

   - **Play greeting phrase to caller when parked**—Select this option to have the system play the greeting phrase you select from the drop-down box, before playing music on hold. Specify whether to play the greeting once only, or every x seconds.

- **Enable Timeout**—Check this box to specify, in seconds, when a line park call will time out. Use the **Timeout option** drop-down boxes to forward the call to the extension that parked the call, alert the extension that parked the call, or forward the call to an AA, voice mail, or an extension/group.
- **Disable ring tone on IP phone when parked by extension**—Check this box to prevent a line-parked call from ringing again while it is parked.

Allow #51 to pick up—when this check box is checked, it allows a user to pick up parked calls from a phone set using **#51**, followed by the Park Line ID.

Deleting a Line Park Group

1. In the **Line Park Configuration** window, select a Line Park Group from the **Groups** list.
2. Click the **Delete** button below the **Groups** list.

CHAPTER

18

Workgroup Configuration

MaxACD for Lync allows up to 64 workgroups to be configured.

When adding members to a workgroup, the following rules apply:

- Concurrent login agent seat license is required.
- One agent login to multiple workgroups requires only one license.
- Each workgroup can have up to 512 members configured.
- A maximum of 256 agents can log in to a workgroup at the same time.
- Per system, a maximum of 256 agent seat licenses can be registered.
- Per system, including all workgroups, a maximum of 1,280 logged-in agents are allowed. (Example: 128 agent seats registered in the system. 256 agents are configured in 10 workgroups but only 128 can be logged in at the same time. Each agent belongs to 10 workgroups. The system has reached the 1,280 logged-in agents limit.)

Workgroup Functionalities

The MaxACD system has the following workgroup functionalities:

System Features

- Call queuing and call distribution
- Define service level threshold and service level calculation methods
- Group busy/RNA/logout handling
- Queue position and expected queue time announcement
- Queue phrase management
- Queue overflow
- Quit queue options
- Workgroup voice mail with forwarding and notification functions
- Agent login/logout management with reason code
- Agent ready/not-ready and wrap-up management
- Record inbound and outbound workgroup calls

- Allow supervisor to redirect call
- Allow supervisor to change call priority in queue
- Define workgroup operation hours and routing
- Auto logout all agents after operation hours
- Priority queuing and call distribution
- Skill-based routing
- Caller selectable information menu while in queue

Agent’s Phone Operation

- Set Login (#54) and Logout (#56)
- Set Ready (#90) and Not Ready (#91)
- Set outbound WG number (#53)

Agent Desktop Application (MaxAgent for Lync)

- Real-time workgroup queue and agent statistics display
- Ability to view and check workgroup voice mail
- Set Login and Logout
- Set Ready and Not Ready
- View and pick up calls in queue
- Calls in queue alert option
- Daily performance summary
- View other agents’ status
- View caller’s IVR data and User Data
- Tag memo to a call

Supervisor’s Phone Operation

- Listen to agent’s conversation with feature code **#59**

Supervisor’s Desktop Application (MaxSupervisor)

- View agent’s state
- Record agent’s conversation
- Manage agent’s login/logout status
- Listen, barge in, or coach agent’s conversation
- View agent’s daily performance statistics
- View group’s real-time status
- View group’s daily operation result
- View calls in queue
- Be alerted to calls in queue
- Change call priority
- Pick and redirect calls in queue

Activity Logging and Reporting

- Workgroup and agent activity logging
- Detail and summary data table
- Support external logger
- Support advanced reporting application - AltiGen's MaxReports

After an agent logs into a workgroup, the following states are tracked:

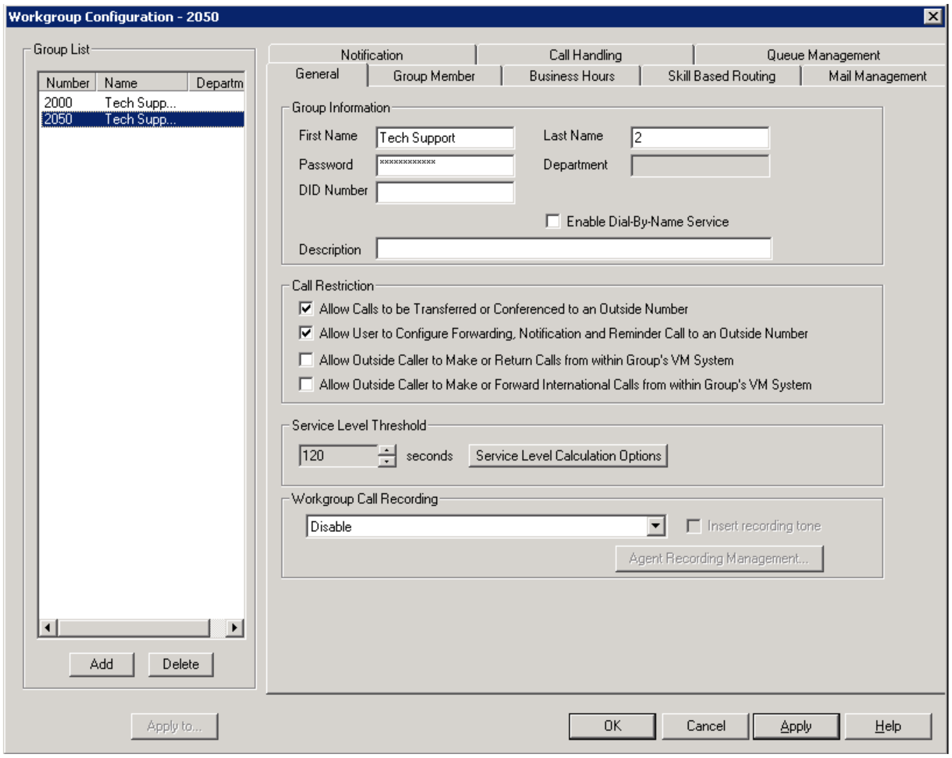
- Idle – The agent's phone is not in use.
- Busy – The agent is connected to a call.
- Wrap-up – The agent enters wrap-up or inter-call delay period. Even if the phone is not in use, the system will mark the agent in wrap-up state.
- Not Ready – The agent changes state to Not Ready.
- DND/FWD – The agent turned on DND or enabled extension forwarding while logged in to a workgroup.
- Error – The agent's phone is off hook for too long, causing the phone to enter an error state.

The priority queuing feature has the following capabilities:

- Tag priority (1-9) to a call entering system. "1" is the highest priority and "9" is the lowest priority.
- Call priority can be set at DNIS Routing, Caller ID Routing, IVR, Advanced Call Router, and SDK.
- If no priority is tagged to a call, the default priority 5 will be assigned to the call before entering a workgroup.
- When a call is in a WG queue, two queue times will be generated. Total queue time will be calculated from the moment the call enters the queue. Priority queue time will be calculated based on the time a call is in queue at a specific priority level. If a priority promotion rule is not enabled, the total queue time will be equal to the priority queue time. If there are multiple calls with the same priority, the call with the longest priority queue time will be served first.
- To prevent calls with lower priority staying in queue forever, causing a high abandon rate, or lowering service level, you can set priority promotion to enhance the caller's position in queue.
- MaxSupervisor can change a call's priority level if the WG's supervisor queue control option is enabled. (Allow Call Redirect/Priority Change)
- When a call's priority is changed, its priority queue time will be reset to 0 and starts accumulating again. For example, caller A with priority 3 has been waiting in the queue for 15 minutes and caller B with priority 2 waiting for 10 minutes. When caller A is promoted to 2, the Priority Queue Time for the caller A is set to 0 and the caller B will be answered first.
- Promoted call priority can be carried to another MaxACD system over VoIP tie trunk.

Creating and Configuring Workgroups

The Workgroup Configuration window provides for creating workgroups, setting their attributes, and assigning group members. To open the Workgroup Configuration window, select **Call Center > Workgroup Configuration**.



Workgroup Configuration - 2050

Group List

Number	Name	Departm
2000	Tech Supp...	
2050	Tech Supp...	

Group Information

First Name: Tech Support
Last Name: 2
Password: ***********
Department:
DID Number:
☐ Enable Dial-By-Name Service
Description:

Call Restriction

☑ Allow Calls to be Transferred or Conferenced to an Outside Number
☑ Allow User to Configure Forwarding, Notification and Reminder Call to an Outside Number
☐ Allow Outside Caller to Make or Return Calls from within Group's VM System
☐ Allow Outside Caller to Make or Forward International Calls from within Group's VM System

Service Level Threshold

120 seconds

Workgroup Call Recording

Disable
☐ Insert recording tone

Figure 18-1. Workgroup Configuration window, General tab

Overview of Workgroup Configuration Window

These are the tabs in the Workgroup Configuration window:

- **General**—create workgroup pilot numbers, group descriptions, service level threshold and call recording options.
- **Group Member**—add or remove members from workgroups
- **Business Hours**—set business hours for workgroups
- **Skill Based Routing**—define skill levels and skill-based routing rules.
- **Mail Management**—set capacity and features options for extension mailboxes.
- **Notification**—set preferences and options for voice mail notifications.
- **Call Handling**—set call forwarding, call waiting, and call handling preferences and options.
- **Queue Management**—set queue phrases, overflow routing, queue announcements and queue quit option.

Apply to Button

The Workgroup Configuration window often allows you to apply changes to a particular workgroup or to select many workgroups to which to apply the changes.

Clicking the **Apply to** button pops up a list of all workgroups to which the change can apply. All workgroups are selected by default. You then de-select the ones you don't want, or de-select all and then select the ones you want. Note that you cannot use the mouse to drag over and select multiple items; you must use the **Shift** and **Ctrl** keys.

The **Apply to** button is disabled unless there is a change that can be applied to multiple workgroups, and when you use it to apply changes to multiple workgroups, it works on only those changed attributes that can be applied.

Setting Up Workgroups

Set up new workgroups in the Workgroup Configuration window.

To create a workgroup:

1. Click the **Add** button under the **Group List**. The **Add New Group** dialog box opens.

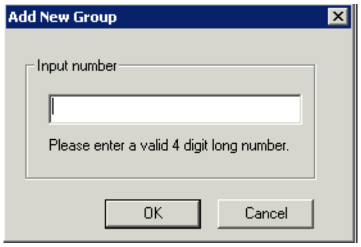


Figure 18-2. Add New Workgroup dialog box

2. Type in a group number for the workgroup.
3. Click **OK**.

Establishing Basic Workgroup Attributes

After you create a workgroup, you can set basic attributes on the Workgroup Configuration **General** tab.

- **First Name** and **Last Name**—each with a maximum of 32 characters.
- **Password**—the default is the system default password set on the **Number Plan** tab of the System Configuration window.

  A valid password cannot be the same as its workgroup number and must be 4–8 digits (numbers or letters A–Z) in length. Basic password patterns, such as repeated digits (1111), consecutive digit strings (1234), or digits that match the extension (Ext. **101** using **101**2, 9**101**, **101**01, etc.) are not recommended. The letters map to numbers (on a phone, for example) as follows:

Numbers	Letters	Numbers	Letters
2	A, B, C, a, b, c	6	M, N, O, m, n, o
3	D, E, F, d, e, f	7	P, Q, R, S, p, q, r, s
4	G, H, I, g, h, i	8	T, U, V, t, u, v
5	J, K, L, j, k, l	9	W, X, Y, Z, w, x, y, z

- **Department**—Departments can be defined and extensions/groups can be assigned to a department by using Enterprise Manager. When this is done, the department is displayed here.
- **DID Number**—each workgroup can be assigned a DID number. This number does not have a fixed length, but the length must be long enough (range 2–16) for the system to match the DID incoming call.
- **Enable Dial-By-Name Service**—check this box to allow callers to search the list by employee name for this workgroup extension.
- **Description**—describe the purpose of this workgroup.

Setting Call Restrictions

The call restriction rules on the **General** tab apply to users making outbound calls from within voice mail and several workgroup settings. These settings do not impact the call restriction settings configured for the workgroup member's extension in Extension Configuration.

- **Allow Calls to be Transferred or Conferenced to an Outside Number**—when checked, the internal extension user can log into this workgroup voice mail, make a call to a second party, then transfer or conference to a third party.
- **Allow User to Configure Notification and Reminder Call to an Outside Number**—This setting regulates voice mail notification and reminder call configuration.
- **Allow Outside Caller to Make or Return Calls from within Group's VM System**—when checked, an outside caller can dial into the system, log in to workgroup voice mail, and make or return calls from the group's voice mail (Zoomerang feature). International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Forward International Calls from within the Group's VM system**—This setting regulates making international calls from voice mail and forwarding to an international number.

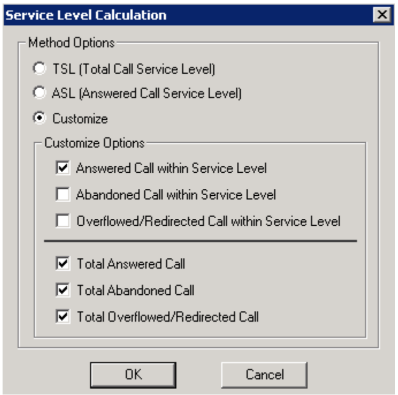
Caution! Allowing any of these options may increase the potential for toll fraud. Make sure the password is properly configured to prevent an intruder from using this voice mail box to make an outbound call. AltiGen recommends that you leave the fourth option unchecked for all workgroups at all times.

Service Level Threshold

The **Service Level Threshold** scroll box allows you to select the length of time in seconds that a call can be in queue before the call is logged in workgroup performance statistics as having exceeded the allowable service level limits. You can set the value to any number between 1–1200 seconds.

Service level is a service quality index which calculates the percentage of calls serviced within a defined threshold for the defined period of time. The term "serviced" may not necessarily mean answered. You can define the calculation method based on your operation requirements. The service level percentage is calculated from midnight 00:00 a.m. and is reset daily. The calculated number will be output to the MaxAgent and MaxSupervisor applications.

The **Service Level Calculations Options** button opens the following dialog box.



Service Level Calculation

Method Options

○ TSL (Total Call Service Level)

○ ASL (Answered Call Service Level)

● Customize

Customize Options

☑ Answered Call within Service Level

□ Abandoned Call within Service Level

□ Overflowed/Redirected Call within Service Level

☑ Total Answered Call

☑ Total Abandoned Call

☑ Total Overflowed/Redirected Call

Figure 18-3. Service Level Calculation dialog box

In the **Method Options** section, select one of the following:

- **TSL** (Total Call Service Level)—the service level calculation is: TSL% = Total WG inbound calls within SLT / Total WG inbound calls. This is the default option.
- **ASL** (Answered Service Level)—the service level calculation is: ASL% = Total WG inbound calls answered within SLT / Total WG inbound calls.
- **Customize**—use the check boxes to enable at least *one* of the following three options:
  - **Answered Calls within Service Level**
  - **Abandoned Calls within Service Level**
  - **Overflowed/Redirected Calls within Service level**

  divided by at least one of the following three options:
  - **Total Answered Calls**
  - **Total Abandoned Calls**
  - **Total Overflowed/Redirected Calls**

Workgroup Recording Options

The system administrator can specify the following *workgroup* call recording options for a workgroup:

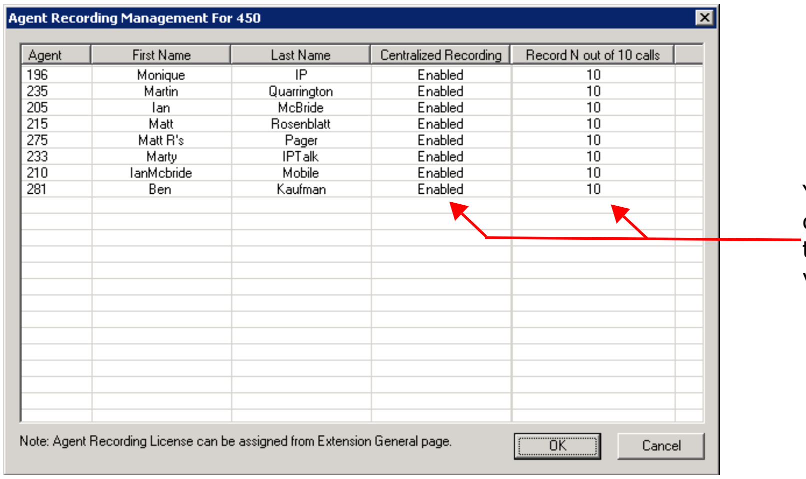
WARNING! Listening in to or recording a conversation without the consent of one or both parties may be a violation of local, state and federal privacy laws. It is the responsibility of the users of this feature to assure they are in compliance with all applicable laws.

- **Disable**—no call recording.
- **Auto record to central location**—records all workgroup inbound and outbound calls, which are saved to a central location (defined in Recording Configuration on the **System** menu—see page "Call Recording Configuration" on page 83); this option requires that a Recording Seat license is assigned to each workgroup member (configured in Extension Configuration).

- **Record on demand to central location**—records calls on demand, which are saved to a central location (defined in Recording Configuration on the **System** menu—see page “Call Recording Configuration” on page 83); this option requires that a Recording Seat license is assigned to each workgroup member (configured in Extension Configuration).
- **Record on demand to extension VM**—records calls on demand, which are saved to the agent’s voicemail box.

  Note: When retrieving voice mail as an e-mail, if the voice mail file has a recorded file attached, the recorded file is not forwarded in the e-mail.
- **Insert Recording Tone**—plays a recording beep to alert the parties that the conversation is being recorded, then plays a periodic recording alert tone. The tone is recorded together with the conversation.
- **Record X out of 10 calls**—If recording to a central location, automatically records incoming and outgoing *workgroup* calls, as specified. (The default is to record all workgroup calls.)

  To see this option, click the **Agent Recording Management** button. This opens the following window:



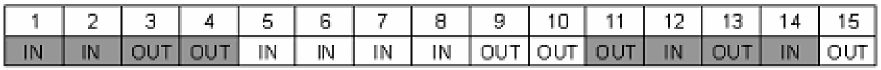
Agent	First Name	Last Name	Centralized Recording	Record N out of 10 calls
196	Monique	IP	Enabled	10
235	Martin	Quarrington	Enabled	10
205	Ian	McBride	Enabled	10
215	Matt	Rosenblatt	Enabled	10
275	Matt R's	Pager	Enabled	10
233	Marty	IPTalk	Enabled	10
210	IanMcbride	Mobile	Enabled	10
281	Ben	Kaufman	Enabled	10

Note: Agent Recording License can be assigned from Extension General page.

You can change these values

Figure 18-4. Agent Recording Management dialog box

For each agent you can change the option **Record N out of 10 calls**. For example, if you set to record 4 out of 10 calls, the 1st-4th and 11th-14th, and so on, will be recorded. Using this example, in the following table the shaded calls will be recorded:



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
IN	IN	OUT	OUT	IN	IN	IN	IN	OUT	OUT	OUT	IN	OUT	IN	OUT

To change **Record N out of 10 calls** for an agent, click the cell you want to change, and make a selection from the drop-down list. Click **Apply**. When finished, click **OK**.

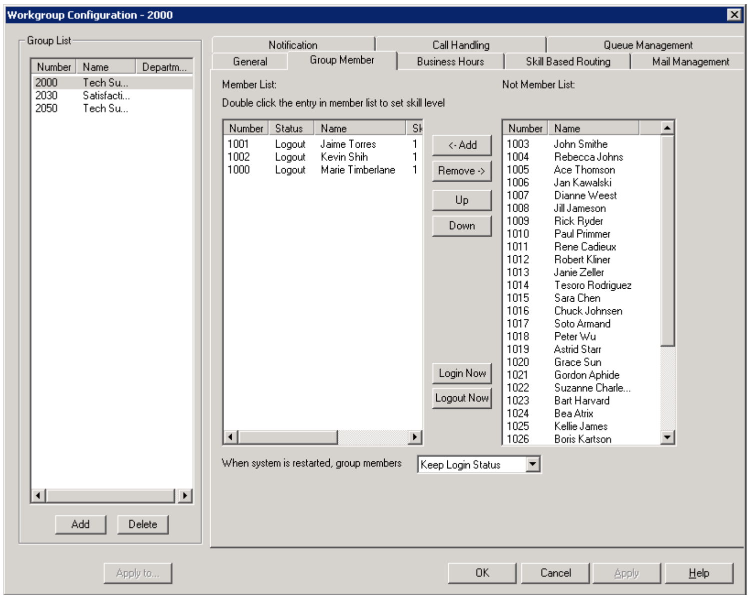
- **Centralized Recording**—You can also enable or disable centralized recording from the Agent Management Recording window shown above. Click the cell you want to change, and make a selection from the drop-down list. Click **Apply**. When finished, click **OK**.

Notes:

- The recording session starts when the call enters the connected state and ends when hang up or flash is pressed, or when the call is transferred.
- When an agent logs in to a workgroup, which is also an outbound workgroup, all outbound calls will be considered as workgroup calls and recorded according to workgroup configuration.
- When an agent logs in to a workgroup and is in Not Ready, DND, Wrap-up, or Inter-call Delay state, outbound calls will be recorded if workgroup recording is configured.
- When an agent does not log in to the workgroup that is configured as an outbound workgroup, all outbound calls are non-workgroup calls.

Establishing Workgroup Membership

Add agent extensions to a workgroup on the **Group Member** tab in the Workgroup Configuration window.



Number	Name	Departm...
2000	Tech Su...	
2030	Satisfacti...	
2050	Tech Su...	

Member List:

Double click the entry in member list to set skill level

Number	Status	Name	Sk
1001	Logout	Jaime Torres	1
1002	Logout	Kevin Shih	1
1000	Logout	Marie Timberlane	1

Not Member List:

Number	Name
1003	John Smithe
1004	Rebecca Johns
1005	Ace Thomson
1006	Jan Kawalski
1007	Dianne Weest
1008	Jill Jameson
1009	Rick Ryder
1010	Paul Primmer
1011	Rene Cadieux
1012	Robert Kliner
1013	Janie Zeller
1014	Tesoro Rodriguez
1015	Sara Chen
1016	Chuck Johnsen
1017	Soto Armand
1018	Peter Wu
1019	Astrid Starr
1020	Grace Sun
1021	Gordon Aphide
1022	Suzanne Charle...
1023	Bart Harvard
1024	Bea Atrix
1025	Kellie James
1026	Boris Kartson

When system is restarted, group members: Keep Login Status

Figure 18-5. Workgroup Configuration, Group Member tab

To add extension(s) to a workgroup:

1. Select the workgroup in the **Group List**.
2. On the **Group Member** tab, click the extension number(s) in the **Not Member** list. Use **Shift**+click and **Ctrl**+click to select several extensions.
3. Click the **Add** button between the columns to move them to the **Member** list.

   Note: If the workgroup pilot extension is configured to Ring All Available Members, the maximum number of members is 20. See “Setting Call Handling Options” on page 171 for details.

   By default, a newly added member has the **Skill Level** set to 1.

4. To change the **Skill Level** designation for a member, double-click the member in the **Member List**. The Skill Level dialog box opens. (Skill Levels are defined in “Setting Up Skill Based Routing” on page 162.)

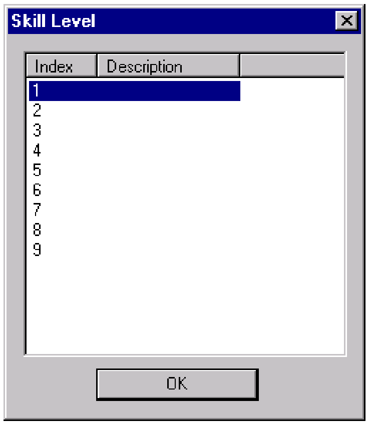


Figure 18-6. Skill Level dialog box

5. Click the desired Skill Level **Index**, then click **OK**.

Agents who are members of more than one workgroup can have a different skill level assigned in each group.

To remove extension(s) from a workgroup:

1. Click the extension number(s) in the **Member** list.
2. Click **Remove** to move them to the **Not Member** list.

Log In/Out a Group Member

An administrator can log in or log out a group member, by selecting the member in the Member List and clicking the **Login Now** or **Logout Now** button.

Setting Login Status for System Restart

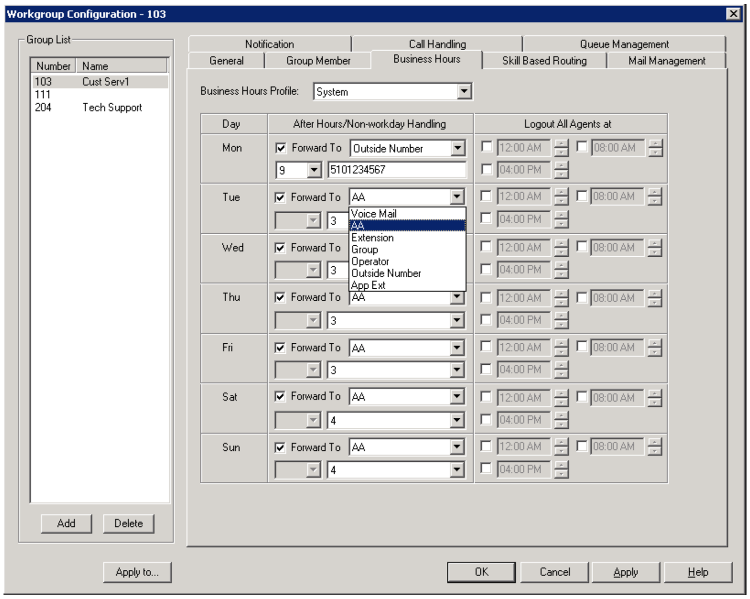
Whenever the system is restarted, the administrator can use the drop-down list at the bottom of the **Group Member** tab to:

- **Keep Login Status**—all group members retain their original login status for that group prior to restart (default setting)
- **All Login**—all group members are automatically logged into the assigned group after the system is restarted.
- **All Logout**—all group members are logged out of the workgroup when the system is restarted.

Setting Business Hours

Settings on the **Business Hours** tab in the Workgroup Configuration window define how after-hours calls are handled for workgroups. An administrator can assign a Business Hours profile to a group, and also configure after-hours handling for each day of the week.

To set after-hours call handling, select the workgroup you want to work with from the **Group List** in the Workgroup Configuration window, then click the **Business Hours** tab.



Number	Name
103	Cust Serv1
111	
204	Tech Support

Business Hours Profile: System

Day	After Hours/Non-workday Handling	Logout All Agents at
Mon	☑ Forward To Outside Number 9 5101234567	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Tue	☑ Forward To AA 3	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Wed	☑ Forward To 3	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Thu	☑ Forward To AA 3	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Fri	☑ Forward To AA 3	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Sat	☑ Forward To AA 4	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Sun	☑ Forward To AA 4	□ 12:00 AM □ 08:00 AM □ 04:00 PM

Figure 18-7. Workgroup Configuration, Business Hours tab

Set the business schedule parameters as follows:

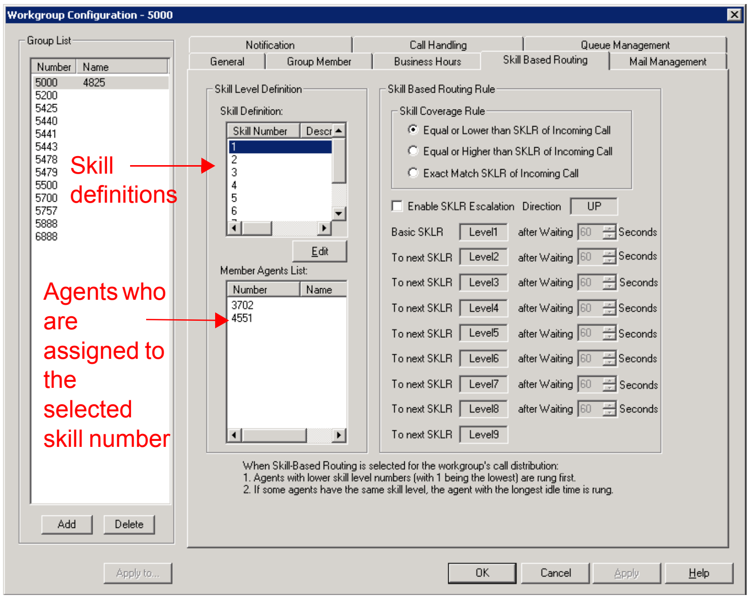
Parameter	Description
Business Hours Profile	Use the drop-down list to select a Business Hours profile to apply to the workgroup (profiles are configured in the System Configuration window—see “Setting Business Hours” on page 39).
After Hours/ Non-Workday Handling	For each day of the week, select a **Forward To** option for call handling after hours or for non-workdays: • To **Voice Mail** • To **AA**—select the auto attendant to use in the drop-down list under the option. AAs are configured in the AA Configuration window, available from the **System** menu. • To an **Extension**—select an extension from the drop-down list. • To a **Group**—select a group from the list. • To the **Operator** • To an **Outside Number**—if you choose **Outside Number**, select a trunk or route access code to use in the small drop-down list on the left, and type in the full prefix and phone number. • To an **App Ext**—when used in conjunction with a third party notification application, the **App Ext** feature enables an extension to connect to an application that can receive the notification event; use the drop-down list to choose the log-on extension to which the third party application is connected. Contact your local AltiGen dealer for more information on using this feature.

Parameter	Description
Logout All Agents At	For each day of the week, you can select up to three time periods for the system to automatically log out agents.

Setting Up Skill Based Routing

If you want to set up skill-based routing, you can more closely match a customer's call to an agent who has the skills needed to handle that customer's issue. Skill-based routing can increase customer issue resolution on the first call, lower the abandoned call rate, and in turn increase customer satisfaction.

The **Skill Based Routing** tab in the Workgroup Configuration window lets you define up to nine different levels of skill needed to handle the variety of a workgroup's calls.



Workgroup Configuration - 5000

Group List

Number	Name
5000	4825
5200	
5425	
5440	
5441	
5443	
5478	
5479	
5500	
5700	
5757	
5888	
6888	

Skill definitions

Agents who are assigned to the selected skill number

Skill Level Definition

Skill Definition:

Skill Number	Descr
1	
2	
3	
4	
5	
6	

Member Agents List:

Number	Name
3702	
4551	

Skill Based Routing Rule

Skill Coverage Rule

● Equal or Lower than SKLR of Incoming Call
○ Equal or Higher than SKLR of Incoming Call
○ Exact Match SKLR of Incoming Call

□ Enable SKLR Escalation Direction UP

Basic SKLR	Level1	after Waiting	60	Seconds
To next SKLR	Level2	after Waiting	60	Seconds
To next SKLR	Level3	after Waiting	60	Seconds
To next SKLR	Level4	after Waiting	60	Seconds
To next SKLR	Level5	after Waiting	60	Seconds
To next SKLR	Level6	after Waiting	60	Seconds
To next SKLR	Level7	after Waiting	60	Seconds
To next SKLR	Level8	after Waiting	60	Seconds
To next SKLR	Level9			

When Skill-Based Routing is selected for the workgroup's call distribution:
1. Agents with lower skill level numbers (with 1 being the lowest) are rung first.
2. If some agents have the same skill level, the agent with the longest idle time is rung.

Figure 18-8. Workgroup Configuration, Skill Based Routing tab

Skill number 1 could define the most basic skill and level 9 the most advanced, or vice versa. Or the skill numbers can be used in any other way that works for the way your company does business.

After skill numbers have been defined on this tab, each agent in the workgroup should be assigned a skill number, according to that agent's knowledge and ability, on the **Group Member** tab.

Incoming calls can be set to ring agents according to skill number, thus more closely directing the caller to an available agent qualified enough to help the caller, but ideally not *over*-qualified. You can determine the skill required by the caller and set the SKLR number in several places:

- The auto attendant, depending on the caller's responses (see "Configuring Menu Items" on page 68)
- The DNIS number the caller dialed, depending on how you have set up your DNIS numbers (see "Configuring DNIS Routing" on page 113)
- The caller ID (see "Configuring Caller ID Routing" on page 110)

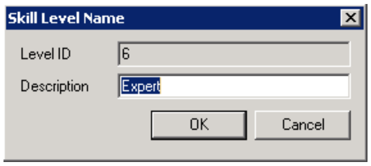
- The Advanced Call Router—You can define SKLR in each rule entry in the Call Router, and if the Call Router routes a call, SKLR will be set.
- In the SDK—A call's SKLR can be set in some modules, and if a call is connected to an App Ext, this App Ext can set or change the call's SKLR

You can set rules on the **Skill Based Routing** tab to allow all calls coming into a workgroup to be handled by agents with a lower skill number or a higher skill number than is set for a call. And you can set time-based rules that alter the call's SKLR to allow either less able agents or over-qualified agents to handle a call so that the caller does not have to wait for an excessive period of time.

Note: For the settings configured on the **Skill Based Routing** tab to take effect, you must select the **Skill-Based Routing** option on the **Call Handling** tab of the Workgroup Configuration window (see "Setting IntraGroup Call Distribution" on page 174).

Defining a Skill for a Workgroup

1. Select a workgroup in the **Group List**.
2. Double-click a skill number in the **Skill Definition** list, or select a skill number and click the **Edit** button.
3. In the **Skill Level Name** dialog box, enter the skill name in the **Description** field, then click **OK**.



Level ID: 6

Description: Expert

Figure 18-9. Skill Level Name dialog box

The description appears in the **Skill Definition** list for that skill number.

Setting Rules for Skill Based Routing

The **Skill Coverage Rule** on the **Skill Based Routing** tab establishes the pool of agents who can handle a particular workgroup call, based on the SKLR setting for that call. The group may comprise:

- Only agents assigned that skill number
- Agents with a given skill number and lower
- Agents with a given skill number and higher

This setting must be configured.

To further help ensure that a workgroup is handling calls in a timely manner, you can specify how many seconds a caller can be in queue before opening the call to agents with the next skill number up or the next skill number down, in successive steps.

To set skill-based routing rules:

1. In the Workgroup Configuration window, **Skill Based Routing** tab, select the workgroup for which you want to set the rules.
2. Select an Agent's Coverage Rule

- **Exact Match SKLR of Incoming Call**

  Only agents whose skill number matches the SKLR of the incoming call can answer the call. For example, if you have three callers with SKLR equal to 2 in the workgroup queue, and all agents with skill level 2 are busy, and there are agents with skill level 1 and 3 who are idle, the system will keep the callers in queue waiting for an agent with skill level 2 to be available.
- **Equal or Lower than SKLR of Incoming Call**

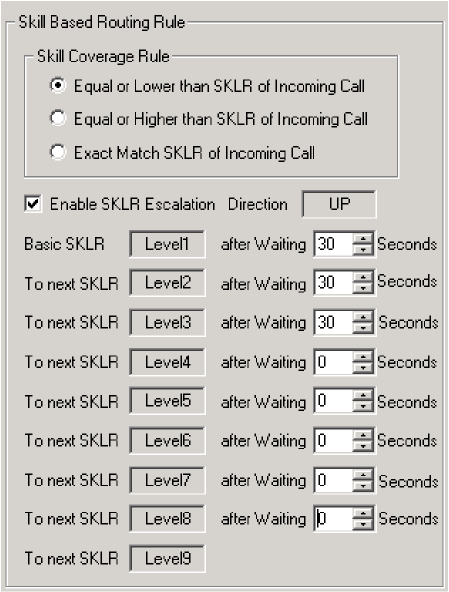
  Any agent whose skill number is equal to or lower than the SKLR of the incoming call may handle this call. Agents with the lowest skill number are rung first. With this option, that would be agents whose skill number is 1. Set the SKLR as if you were setting a ceiling on the resources you are willing to use for this type of call. For example, you can set a regular call's SKLR to 1 and a preferred customer's SKLR to 3. Calls from preferred customers can be answered by agents with skill level 3, 2, and 1 while regular calls can only be answered by agents with skill level 1.
- **Equal or Higher than SKLR of Incoming Call**

  Any agent whose skill number is equal to or higher than the SKLR of the incoming call may handle this call. Agents with the lowest skill number are rung first. With this option, that would be agents whose skill number matches the SKLR. Set the SKLR as if you were setting a minimum skill level requirement for the call. For example, say a technical support group has agents with skill level 1 (beginner), 2 (intermediate), and 3 (expert). If you select the "Equal or Higher" option, calls with SKLR 2 will be queued for an agent with skill level 2 or 3.

3. To increase coverage of calls, check the **Enable SKLR Expansion** check box. (This check box is available if you selected the **Equal or Lower** option or the **Equal or Higher** option.)
4. For each level, specify the number of seconds a call can be in queue before the system will include the next level of agents in the pool of agents who may handle the call. Either use the Up/Down arrows or type in a number from 1-999.

Skill-Based Rule Example 1

Example 1: Coverage rule is **Equal or Lower** and **Enable SKLR Escalation** is checked.



Skill Based Routing Rule

Skill Coverage Rule

● Equal or Lower than SKLR of Incoming Call

○ Equal or Higher than SKLR of Incoming Call

○ Exact Match SKLR of Incoming Call

☑ Enable SKLR Escalation Direction UP

Basic SKLR	Level1	after Waiting	30	Seconds
To next SKLR	Level2	after Waiting	30	Seconds
To next SKLR	Level3	after Waiting	30	Seconds
To next SKLR	Level4	after Waiting	0	Seconds
To next SKLR	Level5	after Waiting	0	Seconds
To next SKLR	Level6	after Waiting	0	Seconds
To next SKLR	Level7	after Waiting	0	Seconds
To next SKLR	Level8	after Waiting	0	Seconds
To next SKLR	Level9			

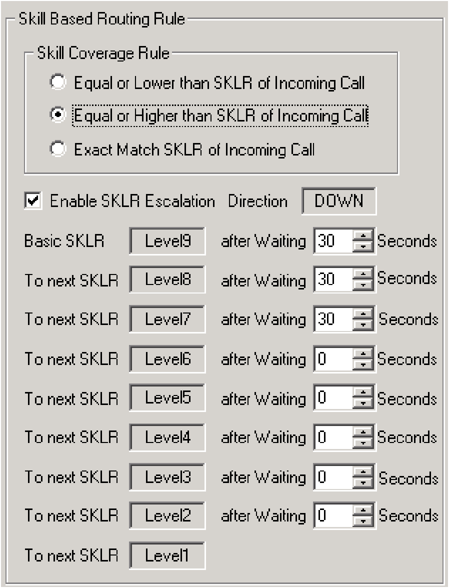
Figure 18-10. Example: Skill-based Routing rules, Equal or Lower

The above configuration means:

1. When a caller with SKLR 1 is waiting in queue for 30 seconds, the caller's SKLR will be escalated to 2. Agents with skill levels 1 and 2 are able to handle the call.
2. If the caller stays in queue for more than 60 seconds, the caller's SKLR will be escalated to 3. Agents with skill levels 1, 2, and 3 are able to handle the call.
3. If the caller stays in queue for more than 90 seconds, the caller's SKLR will be escalated to 9 because all other escalation wait times are set to 0 seconds. The call will be distributed any idle agent in the workgroup.

Skill-Based Rule Example 2

Example 2: Coverage rule is **Equal or Higher** and **Enable SKLR Escalation** is checked.



Skill Based Routing Rule

Skill Coverage Rule

○ Equal or Lower than SKLR of Incoming Call

● Equal or Higher than SKLR of Incoming Call

○ Exact Match SKLR of Incoming Call

☑ Enable SKLR Escalation Direction DOWN

Basic SKLR	Level9	after Waiting	30	Seconds
To next SKLR	Level8	after Waiting	30	Seconds
To next SKLR	Level7	after Waiting	30	Seconds
To next SKLR	Level6	after Waiting	0	Seconds
To next SKLR	Level5	after Waiting	0	Seconds
To next SKLR	Level4	after Waiting	0	Seconds
To next SKLR	Level3	after Waiting	0	Seconds
To next SKLR	Level2	after Waiting	0	Seconds
To next SKLR	Level1			

Figure 18-11. Example: Skill-based Routing rules, Equal or Higher

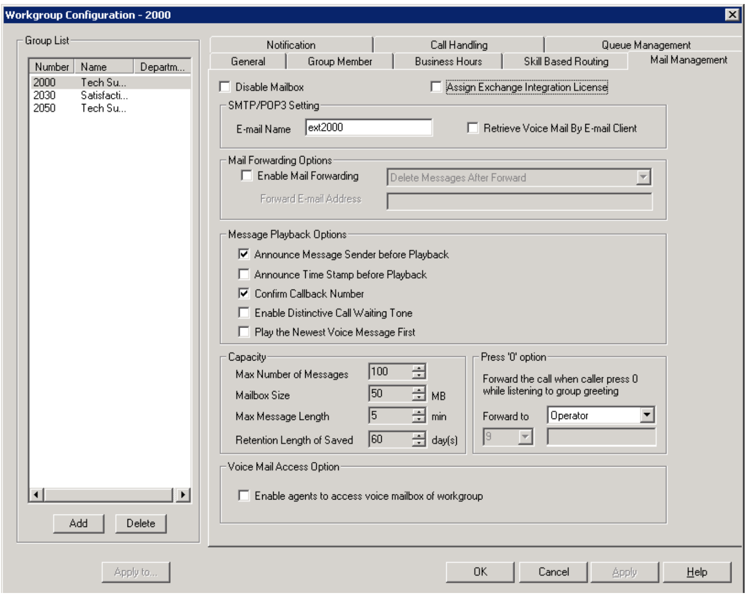
The above configuration means:

1. When a caller with SKLR 9 waiting is in queue for 30 seconds, the caller's SKLR will be changed to 8. Agents with skill level 8 and 9 are able to handle the call.
2. If the caller stays in queue for more than 60 seconds, the caller's SKLR will be changed to 7. Agents with skill level 7, 8, and 9 are able to handle the call.
3. If the caller stays in queue for more than 90 seconds, the caller's SKLR will be escalated to 1 because all other escalation wait times are set to 0 seconds. The call will be distributed to any idle agent in the workgroup.

Setting Workgroup Mail Management

The Mail Management settings define how voice messages are handled for a workgroup, including how messages are announced and processed, and how much capacity is allotted to message storage.

To work with mail management settings, click the **Mail Management** tab, and select the workgroup number you want to work with from the **Group List**.



Workgroup Configuration - 2000

Group List

Number	Name	Departm...
2000	Tech Su...	
2030	Satisfacti...	
2050	Tech Su...	

□ Disable Mailbox
□ Assign Exchange Integration License

SMTP/POP3 Setting

E-mail Name: ext2000
□ Retrieve Voice Mail By E-mail Client

Mail Forwarding Options

□ Enable Mail Forwarding — Delete Messages After Forward
Forward E-mail Address:

Message Playback Options

☑ Announce Message Sender before Playback
□ Announce Time Stamp before Playback
☑ Confirm Callback Number
□ Enable Distinctive Call Waiting Tone
□ Play the Newest Voice Message First

Capacity

Max Number of Messages: 100
Mailbox Size: 50 MB
Max Message Length: 5 min
Retention Length of Saved: 60 day(s)

Press '0' option

Forward the call when caller press 0 while listening to group greeting
Forward to: Operator
9

Voice Mail Access Option

□ Enable agents to access voice mailbox of workgroup

Figure 18-12. Workgroup Configuration, Mail Management tab

Note: You can use **Apply to** to apply mailbox settings to one, some, or all workgroup.

Disabling a Mailbox

When you disable a mailbox, the normal greeting is played but callers cannot leave messages.

Setting E-mail Options

On the **Mail Management** tab, you can set the e-mail options for the workgroup:

- **E-mail Name**—the workgroup's e-mail name without the @domain. The default e-mail name is `ext`<*workgroup number*>*,* that is, the letters "ext" followed by the workgroup number. For example, the default e-mail name for workgroup 5000 would be **ext5000**.
- **Retrieve Voice Mail by E-mail Client**—selected, this sends voice mail to the user extension as an e-mail attachment. Deselected, voice mail is retrieved as voice mail.
- **Enable Mail Forwarding**—selected, the workgroup's e-mail will be forwarded to the e-mail address you specify in the **Forward E-mail Address** box. The address should be a full address, including the domain (for example, *jsmith@thecompany.com*).

  If you enable mail forwarding, you also specify what you want done with the original messages after they have been forwarded. In the drop-down list you can choose to:

  - Delete Messages after Forward
  - Keep the Messages as New
  - Keep Messages as Saved

Setting Mailbox Playback Options

You can use the following check boxes to turn on or off options for listening to playback of recorded messages. These options apply to both new messages and saved messages, and they can be applied to multiple workgroups using **Apply to**:

Parameter	Description
Announce Message Sender Before Playback	Selected, the user hears the name of the message sender (internal sender only) before listening to recorded AltiGen Voice Mail System messages.
Announce Time Stamp Before Playback	Selected, the user hears the timestamp (time and date) of each message before playback.
Confirm Callback Number	Selected, system confirms the accuracy of the caller's number.
Enable Distinctive Call Waiting Tone	Selected, the user hears three different call waiting tone cadences to distinguish between internal, external, and operator calls.
Play the Newest Voice Message First	Selected, new voice mail will be retrieved first. When not selected, the system will play voice mail based on FIFO (first in, first out).

Setting Mailbox Capacities

You can set various mailbox capacities with the following options, and you can apply the settings to multiple workgroups using **Apply to**:

Parameter	Description
Max Number of Messages	Maximum number of messages stored in the workgroup's mailbox. The range is **1**–**999**, defaulting to 100.
Mailbox Size	Mailbox size in MBs of stored messages. The range is **1**–**500** MB, with a default of 50.
Max Message Length	Maximum length of voice messages in minutes. The range is **1**–**30** minutes, with a default of 5 minutes.
Retention Length of Saved	Number of days saved messages are archived by the system. The range is **1**–**90** days, with a default of 60.

Press Zero Option

This option allows a caller to press "0" while listening to this workgroup's greeting. When the caller presses "0," the call will forward to the specified destination. Use the drop-down list to spedify a forwarding destination for the call: **Voice Mail**, **AA**, **Extension**, **Group**, **Operator** (default), **Outside Number**, **App Ext**, or **Line Park**.

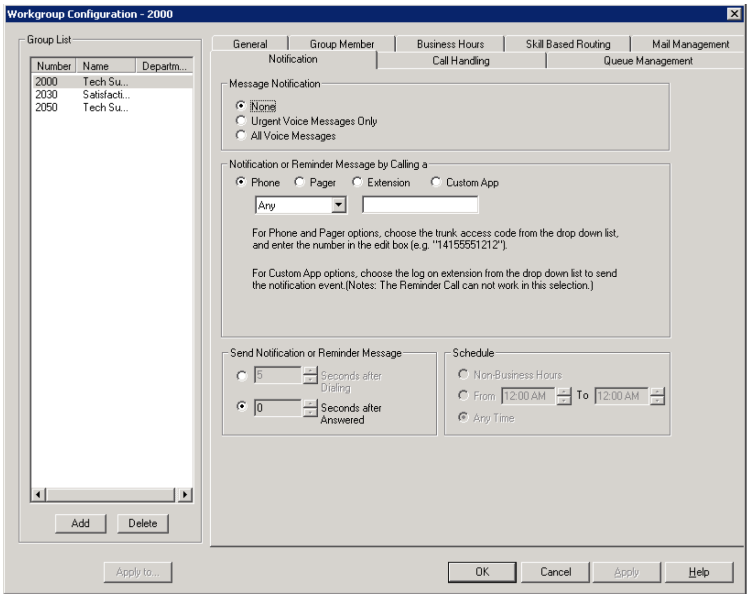
If you choose to forward to an **Outside Number**, select a trunk or route access code to use in the small drop-down list on the left, and type in the full prefix and phone number.

Voice Mail Access Option

To allow agents of a workgroup to access the group's voice mail in MaxAgent (MaxAgent's **WG Voicemail** tab), select the group and check **Enable agents to access voice mailbox of workgroup**.

Setting Message Notification Options

To set notification options on new incoming e-mail and voice messages, click the **Notification** tab in the Workgroup Configuration window, and select the workgroup number from the **Group List**.



Group List

Number	Name	Departm...
2000	Tech Su...	
2030	Satisfacti...	
2050	Tech Su...	

Message Notification

● None
○ Urgent Voice Messages Only
○ All Voice Messages

Notification or Reminder Message by Calling a

● Phone ○ Pager ○ Extension ○ Custom App

Any

For Phone and Pager options, choose the trunk access code from the drop down list, and enter the number in the edit box (e.g. "14155551212").

For Custom App options, choose the log on extension from the drop down list to send the notification event.(Notes: The Reminder Call can not work in this selection.)

Send Notification or Reminder Message

○ 5 Seconds after Dialing
● 0 Seconds after Answered

Schedule

○ Non-Business Hours
○ From 12:00 AM To 12:00 AM
● Any Time

Figure 18-13. Workgroup Configuration, Notification tab

Individual users can also configure **Message Notification** within the AltiGen Voice Mail System.

Note: You can use **Apply to** to apply mailbox settings to one, some, or all workgroups. See "Apply to Button" on page 154 for more information on using **Apply to**.

Setting the Message Types for Notification

Select the types of messages for which the workgroup user will be notified:

- **None**—selected, the user is *not* notified with a call regarding newly received messages. Selecting this option does not prevent the user from getting message waiting indicators or stutter dial tone when new messages are received.
- **Urgent Voice Messages Only**
- **All Voice Messages**

Please note that the system will start notification as soon as it enters non-business hours under the following conditions:

- Extension is set to notify **Urgent Voice Message Only**

- Notification is set to **Non-Business Hours**
- Voice mail is received during business hours and is marked urgent
- Extension user does not check the urgent message

Setting the Type of Notification

There are four options for sending the notification or reminder message: **phone**, **pager**, **extension** or **custom application (Custom App)**.

- **Extension** - to use the Extension option, select the **Extension** radio button, then type the extension number into the text box.
- **Phone/Pager** - for the **Phone** and **Pager** options, first specify the trunk or route access code using the drop-down list next to the **Phone** radio button. The **Any** option means to locate any available trunk. Then type in the number with all relevant dialing prefixes other than the trunk code, using a maximum of 63 digits.
- **Custom App** - when used in conjunction with a third-party notification application, the **Custom App** feature enables an extension to connect to an application that can receive the notification event; use the drop-down list to choose the log-on extension to which the third-party application is connected. Contact your local AltiGen dealer for more information on using this feature.

  Note: The Reminder Call will not work with this selection.

Note also the following considerations:

- For the **Pager** option, the system calls the specified pager number and then dials the system main number (as set in System Configuration, **General** tab), which is then displayed on the user’s pager.

  For the operator-assisted paging function, the operator phone number **and** the pager number must be entered in the **<phone number>*<pager number>** format. For example, if the phone number to call the pager operator is **7654321** and the pager number to page the user is **12345678**, the notification outcall number that needs to be entered is **7654321*12345678**. When the pager operator answers the Message Notification call, MaxACD announces the **pager number and** the **System Main Number** (as configured on the **General** tab of **System Configuration**), which will be displayed on the user’s pager. The operator is also given the option to repeat these numbers by pressing ‘**#**’.

Outcall to Cellular or PCS Phone Numbers

When an outcall is made by the system (for Message Notification, Zoomerang, Call Forwarding, and so on) to a cellular or PCS phone, it may ring the phone once but not necessarily present the call and make a connection. This will happen if the ringback tone played by the cellular service provider does not conform to standard ringback tones. To work around this problem, append a few commas (**,**) to the outcall (cellular) number when entering it. Each comma provides a one second pause.

Setting Notification Timing

When notification is configured to an *outside phone number*, the system will announce, "This is the outcall notification message for…" after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the carrier. If the system plays the announcement phrase before the notification call is answered, the phrase will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing—**If the carrier of the outside phone number cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)

  Note: Note: If the delay is set too long, the notified party will hear silence before the announcement is played.

- **Seconds after Answered—**This field is set to 0 seconds and it is not configurable for notification to a phone number. It means the system will play the announcement immediately after answer supervision is received.

When notification is configured to a *pager*, the system will transmit DTMF digits as the return phone number (the **System Main Number** as set in the System Configuration **General** tab) after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the pager system. If the system sends digits before the call is connected, some digits will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing—**If the pager carrier cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)
- **Seconds after Answered—**If the answer supervision signal is provided by the carrier, check this option and set the delay timer to 2 to 5 seconds. In some cases, the pager carrier cannot detect DTMF right after the call connection. (Default is 10 seconds, maximum is 30.)

  Note: You may need to try a different delay setting to make sure the user return number is transmitted properly after configuration.

Setting Notification Business Hours

You can choose one of three options for when the extension user is to be notified of new messages:

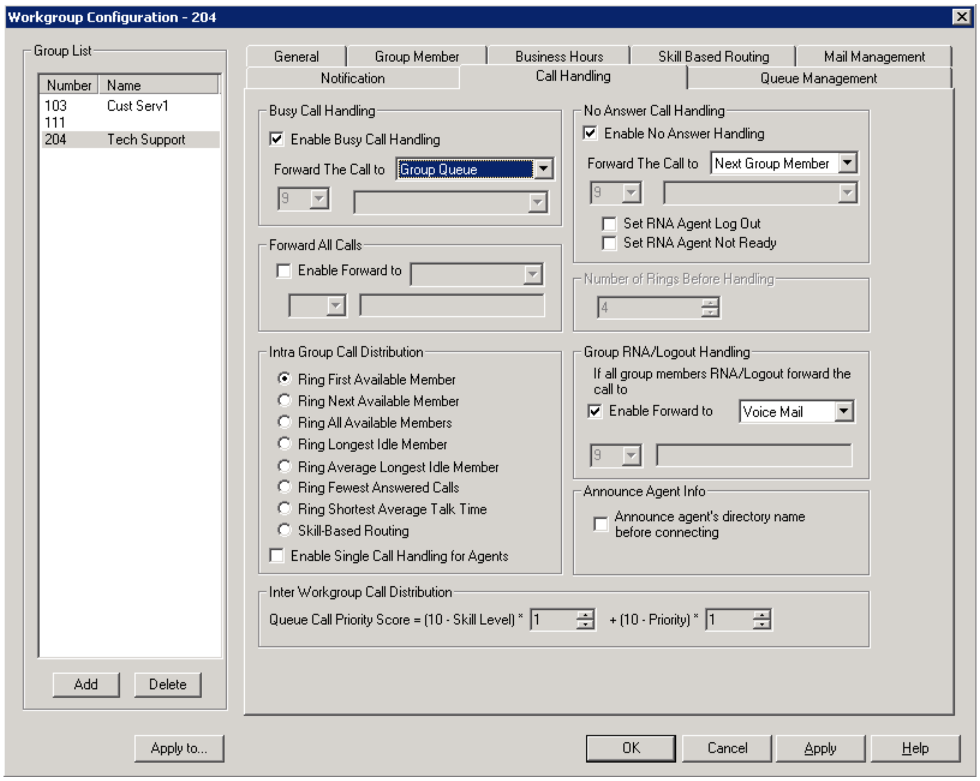
- **Non-Business Hours**—notification only during non-business hours. Business hours are set in System Configuration, **Business Hours** tab (see "Setting Business Hours" on page 39).
- **From/To**—notification during a specified time of day*.* Select the hours in the **From** and **To** time scroll boxes.
- **Any Time**—notification at all times (every day).

Setting Call Handling Options

Call Handling options include forwarding, handling busy calls, handling no-answers and other options.

You can use **Apply to** to apply call restriction settings to one, some, or all workgroups.

To work with workgroup call handling options, click the **Call Handling** tab in the Workgroup Configuration window, and select the workgroup number from the **Group List**.



Workgroup Configuration - 204

Group List

Number	Name
103	Cust Serv1
111	
204	Tech Support

Busy Call Handling
☑ Enable Busy Call Handling
Forward The Call to: Group Queue

Forward All Calls
☐ Enable Forward to

Intra Group Call Distribution
● Ring First Available Member
○ Ring Next Available Member
○ Ring All Available Members
○ Ring Longest Idle Member
○ Ring Average Longest Idle Member
○ Ring Fewest Answered Calls
○ Ring Shortest Average Talk Time
○ Skill-Based Routing
☐ Enable Single Call Handling for Agents

No Answer Call Handling
☑ Enable No Answer Handling
Forward The Call to: Next Group Member
☐ Set RNA Agent Log Out
☐ Set RNA Agent Not Ready

Number of Rings Before Handling: 4

Group RNA/Logout Handling
If all group members RNA/Logout forward the call to
☑ Enable Forward to: Voice Mail

Announce Agent Info
☐ Announce agent's directory name before connecting

Inter Workgroup Call Distribution
Queue Call Priority Score = (10 - Skill Level) * 1 + (10 - Priority) * 1

Figure 18-14. Workgroup Configuration, Call Handling tab

Handling Busy Calls

You have several options for handling calls when the workgroup extension is busy. If you do not enable busy call handling, the caller simply hears a busy signal.

To enable the options, select the **Enable Busy Call Handling** check box, then select from the following forwarding options:

- **Group Queue**—The caller will stay in the workgroup queue waiting for any agent to become available. If there is no agent logged in at this moment, the system will use **Group Logout Handling** to handle this call.
- **Group Voice Mail**
- **AA**—forward caller to an auto attendant.
- **Extension**—forward caller to an extension.
- **Group**—forward caller to another group.
- **Line Park**—forward caller to a Line Park group.

Forwarding All Calls

When you do not want the workgroup to handle any calls, check the **Enable Forward To** option in the Forward All Calls section of the **Call Handling** tab, and select an option.

The forwarding options are as follows:

- To **Voice Mail**

- To an **Extension**—select an extension number in the drop-down list.
- To **AA**—select the AA to use in the drop-down list below the option.
- To a **Group**—select a group from the drop-down list.
- To the **Operator**
- To an **Outside Number**—this option is available if it is allowed in the **Other Call Restrictions** option in the **Restriction** tab, as discussed in "Setting Other Call Restrictions" on page 138. Also, see "Outcall to Cellular or PCS Phone Numbers" on page 170.
- If you choose **Outside Number**, select a trunk or route access code to use in the small drop-down list on the left, and type in the full prefix and phone number.
- To an **App Ext**—when used in conjunction with a third-party notification application, the **App Ext** feature enables an extension to connect to an application that can receive the notification event; use the drop-down list to choose the log-on extension to which the third-party application is connected. Contact your local AltiGen dealer for more information on using this feature.
- To **Line Park**—if configured, select a **Line Park** group from the drop-down list.

Handling Unanswered Calls

The **Enable No Answer Handling** configuration provides options for handling calls when the system rings the first available agent and the call is not answered. If *all* agents in the workgroup are rung and no one answers the call, the system will use the Group RNA/Logout Handling rule. **Enable No Answer Handling** is not available if Intra Group Call Distribution is set to **Ring All Available Members**.

To configure this option, check the **Enable No Answer Handling** box.

Select one of the following forwarding options for no answer call handling:

- **Next Group Member** - ring the next available agent until all available agents are rung. If all agents are busy, caller will stay in the workgroup queue.
- **Extension** - take the call out of the workgroup and forward it to an extension.
- **Group** - take the call out of workgroup and forward it to another group.
- **Group Voice Mail** - transfer the caller to the workgroup voice mail when the first available agent does not answer the call.
- **Member Voice Mail** - transfer the caller to the first available agent's voice mail if this agent does not answer the call.
- **AA** - take the call out of the workgroup and forward it to an auto attendant.
- **Line Park** - take the call out of the workgroup and forward it to a Line Park group.

Set RNA Agent Auto Logout Check Box

Select this option to have the system automatically log out an agent extension from a workgroup if RNA is encountered.

Set RNA Agent Not Ready Check Box

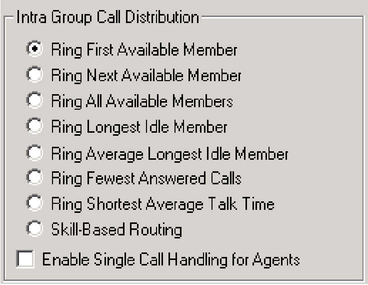
Select this option to have the system automatically set an agent's extension in a workgroup to not ready if RNA is encountered.

Number of Rings Before Handling

If you select **Ring All Available Members** in the Intra Group Call Distribution section, then specify the **Number of Rings before Handling**, using the scroll box beside that option. The number of rings is the total number of times agents are rung before the call is handled by the Group RNA/Logout Handling configuration

Setting IntraGroup Call Distribution

The IntraGroup Call Distribution options let you set the handling of normal inbound calls: how to route the incoming call to a workgroup agent, using one of the following options:



Intra Group Call Distribution

● Ring First Available Member
○ Ring Next Available Member
○ Ring All Available Members
○ Ring Longest Idle Member
○ Ring Average Longest Idle Member
○ Ring Fewest Answered Calls
○ Ring Shortest Average Talk Time
○ Skill-Based Routing
□ Enable Single Call Handling for Agents

Figure 18-15. IntraGroup Call Distribution dialog box

- **Ring First Available Member**—first *available* extension in a workgroup. For example, if there are three member extensions in a workgroup, the call is always sent to the *first* member configured in the workgroup. If this member is busy, the call goes to the *second* member configured and so forth.
- **Ring Next Available Member**—a round-robin method that attempts to evenly distribute calls among the group members. This method sends the call to the *next* member configured in a workgroup (regardless of whether the previous member is busy or not). In other words, if the previous call was sent to #3 in the group, the present call is sent to #4, if #4 is not busy.
- **Ring All Available Members**—all extensions in a workgroup.

  Note: When this option is enabled, a single workgroup can have no more than 20 members.

  In addition, calls to the workgroup with this option enabled have higher priority than other workgroup calls. Therefore, if an agent belongs to multiple workgroups, one of which has this option enabled, a call to that workgroup will be processed first, regardless of Wait Time of calls in other workgroups which are not set to Ring All.

  If members are using IP extensions, the system will not use the IP codec channel during ringing all IP phones. Only one codec will be used when a member of a workgroup answers the call.
- **Ring Longest Idle Member**—The agent who has the longest idle time, defined as follows:
  - The agent needs to be in login state
  - Idle time is calculated from the end of the last wrap-up event.
  - If the agent does not have wrap-up time configured, the idle time is calculated from the end of last busy state.

- **Ring Average Longest Idle Member**—the agent who averages being off the phone the longest:

  ```
  Average Idle Time = (Total Login Time - Total Talk Time) / Total
  Calls Handled
  ```

  - Total Login Time = Cumulative WG login time since midnight
  - Total Talk Time = Cumulative WG Inbound + Outbound call duration since midnight
  - Total Calls Handled = Total number of WG calls (Inbound + Outbound) handled by the agent since midnight

  If a new agent logs into a WG that has been operating for several hours, this agent will have the highest priority to take the call.

  If multiple agents log into a WG that has been operating for several hours, the one with the longest idle time since login will have the highest priority to take the call.

- **Ring Fewest Answered Calls**—the agent who has answered the fewest number of calls.
- **Ring Shortest Average Talk Time**—the agent who averages the shortest talk time.

  Note: Average talk time is calculated as follows:

  ```
  Average Talk Time (ATT) = Total Inbound Talk Time / Total
  Inbound Calls Answered
  ```

  The agent calculated with the lowest value for ATT is rung first.

- **Skill-Based Routing**—the call will be routed according to the SKLR setting and skill-based routing rules set up on the Skill Based Routing tab in the Workgroup Configuration window (see "Setting Up Skill Based Routing" on page 162). When **Skill-Based Routing** is selected, the agent with longest idle time will be selected to take the call when multiple agents with the same skill level are idle.

Enable Single Call Handling for Agents

Check this check box to enable single call handling for workgroup agents.

Note: If single call handling is *enabled* and the agent has one or more calls on hold, MaxACD will not distribute the call to this agent. If single call handling is *disabled*, MaxACD will distribute calls to this agent even when one or more calls are put on hold by this agent.

Handling Calls when Group Members Are RNA/Logged Out

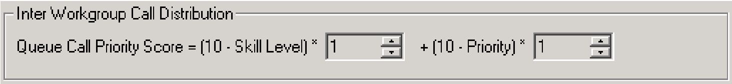
You can set calls to forward to a specified destination when all group members either do not answer the call (RNA) or are logged out. To do so, in the **GroupRNA/Logout Handling** section of the **Call Handling** tab, check the **Enable Forward to** check box, and select a destination from the drop-down list. The forwarding options are the same as for "Forwarding All Calls" on page 172.

Announce Agent Info

Check this check box to have the system announce the agent's directory name before an incoming workgroup call is transferred to an agent from the queue.

Inter Workgroup Call Distribution

In the case where an agent belongs to multiple workgroups and there are queued calls in two or more of these workgroups, as soon as the agent becomes available, the queued call that will be distributed to this agent is determined by the **Inter Workgroup Call Distribution** setting.



Inter Workgroup Call Distribution

Queue Call Priority Score = (10 - Skill Level) * 1 + (10 - Priority) * 1

This field is used to calculate the score of each call in a workgroup’s queue. Depending on the call’s assigned priority and the skill of the agent that is available, the score will determine which workgroup’s call gets answered first. The call with the highest score is answered first. Use the up/down arrows to increase or decrease the weight values for **Priority** and **Skill** values.

The first box is the weight for agent skill in a workgroup. The second box is the weight for priority of a queued call. The score is calculated as (10 - skill level) x weight for agent skill + (10 - queued call priority) x weight for call priority. When determining which call should be dispatched to an idle agent who is assigned to multiple workgroups, the system will consider the following factors:

- Caller's priority
- Agent's skill level
- Caller's SKLR
- Caller's wait time in queue

Configuration Guidelines:

- Assuming an agent is assigned with different skill levels for different workgroups, and call priority is the same for all calls, you can increase the skill weight to 9 and reduce the priority weight to 1 to better match an agent's skill.
- Assuming each call is assigned with a priority based on certain customer attributes, and an agent's skill is the same for all workgroups, you can increase the priority weight to 9 and lower the skill weight to 1 to have a call with higher priority answered first.
- Assuming all calls' priority is the same and agent's skill level is the same for all workgroups, you can use this scoring system to prioritize workgroups. For example, assign priority weight 9 to the most important group, 5 to the second most important group, and 1 to the least important group. Calls in the group with higher priority weight will be dispatched first.
- When there are callers with the same score in different workgroups, the queue time will be used as a tie breaker.
- If you have variable priority settings for callers, and agents belong to multiple workgroups with different skill levels, it is recommend that you set all calls' SKLR to 1 and set call coverage rule to "Equal or Lower than SKLR of Incoming Call". This will eliminate the complexity of matching caller's SKLR to agent's skill level.

Queue Management - Basic

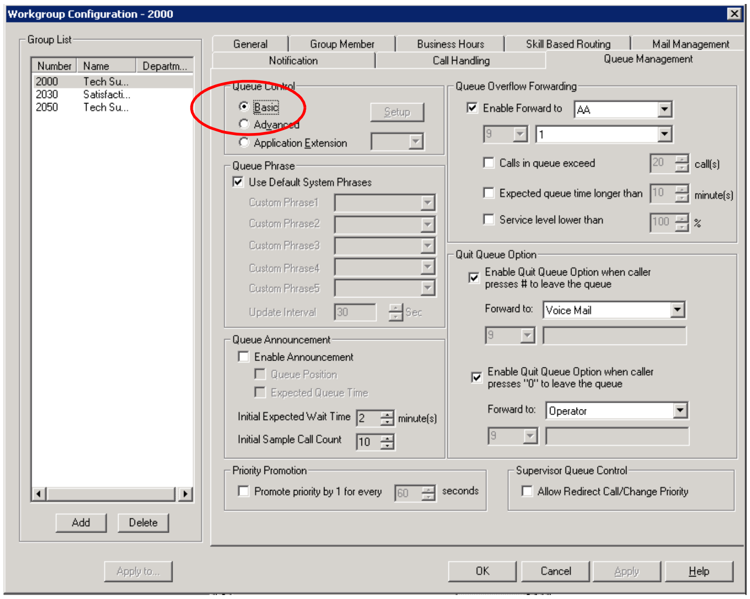
The main differences between Basic and Advanced queue control are the following:

- You can build a layer of DTMF menu selection option in the Advanced queue control mode. A caller can press a digit to hear different prompts or options while in queue.

- You can have select FIFO (First In First Out) or LIFO (Last In First Out) for the queue overflow.

If you don't have these particular needs, the Basic queue mode is recommended.

The **Queue Management** tab in Workgroup Configuration allows you to set options for queue phrases and announcements, queue overflow routing and quit queue options. Options become enabled depending on the Queuing Control selected—**Basic**, **Advanced** and **Application Extension**.



Workgroup Configuration - 2000

Group List

Number	Name	Departm...
2000	Tech Su...	
2030	Satisfacti...	
2050	Tech Su...	

Queue Control

● Basic
○ Advanced
○ Application Extension

Queue Phrase

☑ Use Default System Phrases

Update Interval 30 Sec

Queue Announcement

□ Enable Announcement
□ Queue Position
□ Expected Queue Time

Initial Expected Wait Time 2 minute(s)
Initial Sample Call Count 10

Priority Promotion

□ Promote priority by 1 for every 60 seconds

Queue Overflow Forwarding

☑ Enable Forward to AA
9 1
□ Calls in queue exceed 20 call(s)
□ Expected queue time longer than 10 minute(s)
□ Service level lower than 100 %

Quit Queue Option

☑ Enable Quit Queue Option when caller presses # to leave the queue
Forward to: Voice Mail
9

☑ Enable Quit Queue Option when caller presses "0" to leave the queue
Forward to: Operator
9

Supervisor Queue Control

□ Allow Redirect Call/Change Priority

Figure 18-16. Workgroup Configuration, Queue Management tab, Basic Queue Control

When **Basic** is selected in the **Queuing Control** field, the following queue management options are available:

Setting Queue Phrase Options

For each workgroup, you can either use the system default phrases or you can set up a custom configuration.

The default audio phrases are discussed in “Audio Peripheral Configuration” on page 50.

Queue Announcement

You can set up the system to announce a caller’s queue status—queue position and expected queue time—when an incoming call enters a workgroup queue. To enable this option, check **Enable Announcement**, then check **Queue Position** and/or **Expected Queue Time**.

Queue Position - When checked, the system will tell the caller which position the caller is at in queue. Do not check this option if you assign different priorities to different calls based on DNIS, CID, or AA selection. Do not check this option if you configure matching a caller’s SKLR to an agent's skill level. Queue position is not meaningful when a higher priority caller can push a lower priority caller or if no agent is available to answer a particular SKLR.

Expected Queue Time - when checked, the system will tell the caller how long the wait is expected to be. When calculating this number, the system will consider the average agent call handling time and the position of the caller in queue. Because queue position is a factor when calculating this number, do not check this option when call priority and caller SKLR matching are configured. Please note that the Expected Queue Time is an estimated number. Agents logging in or out of the workgroup during operation hours will affect the actual handling time and cause deviation to the expected queue time.

`Expected Queue Time` (round up to minutes) `= [(Average Call Handling Time x Queue Position) + 59 sec] / 60 sec`

Expected Wait Time Sampling

To calculate Expected Queue Time, the system needs to take samples when a workgroup starts operation. You can set the following parameters to set a sampling period and a fixed Expected Queue Time announcement during sampling period. The expected queue time counter is reset for all workgroups daily at midnight.

- **Initial Sample Call Count** [1 to 100] - How many calls you would like to use as initial samples.
- **Initial Expected Wait** (Queue) **Time** [1 to 10 minutes] - This field defines the expected queue time to be announced during the sampling period.

Queue Overflow Forwarding

The Queue Overflow Forwarding options are for handling long queues or long wait times for callers. When a queue exceeds a set number of calls, or callers are waiting beyond a set length of time, calls can be automatically forwarded to a voicemail box, AA, extension, group, operator, outside number, or application extension.

To set options for handling queue overflow:

1. In the **Queue Overflow Forwarding** section, set options for:
   - **Calls in queue exceed** - when the number of calls in queue are greater than the defined number, new incoming calls will be overflowed to the defined target.
   - **Expected queue time longer than** - when the longest queue time is greater than the specified number of minutes, new incoming calls will be overflowed to the defined target.
   - **Service level lower than** - this number is not a historical service level defined in the workgroup threshold. This number is a real-time queue service level (RTSL) calculated as follows:

     `RTSL% = 1 - (# of queued calls exceed SL threshold / Total calls in queue)`
2. Check the **Enable Forward to** check box and from the drop-down list, select the forwarding destination list to use if the queue length, wait time or service level settings are exceeded. If this option is not checked, calls will go to the workgroup’s voicemail.

Quit Queue Option

The quit queue feature gives a caller the option of leaving a workgroup queue at any time by pressing **#** and/or **0**. To enable this feature, check either or both of the **Enable Quit Queue Options**, then use the appropriate **Forward to** drop-down list to select the option the caller will have:

- **Voice Mail**
- **AA**—select the auto attendant to use. AAs are configured in **AA Configuration** on the **System** menu.
- **Extension**—select an extension from the drop-down list.

  Note: If the forwarding extension is busy when a caller quits a queue, the call will go to this extension’s voice mail.
- **Group**—select a workgroup from the drop-down list.
- **Operator**
- **Outside Number**—this option is available if it is allowed in the **Other Call Restrictions** option in the **Restriction** tab, as discussed in “Setting Other Call Restrictions” on page 138.

  If you choose **Outside Number**, select a trunk or route access code to use in the small drop-down list on the left, and type in the full prefix and phone number.

  Note: Forwarding calls to a pager is possible but *not recommended* since callers will only hear what is heard when calling a pager and will not know to enter a return phone number unless instructed.
- **App Ext**—when used in conjunction with a third-party notification application, this feature enables an extension to connect to an application that can receive the notification event; use the drop-down list to choose the log-on extension to which the third-party application is connected. Contact your local AltiGen dealer for more information on using this feature.
- **Callback Interview**—the System will record the caller’s callback number and will prompt the caller to record a message into the voice mail box of the workgroup.

  Note: This option is only available to external callers.

Priority Promotion

To prevent calls with lower priority staying in queue forever, causing high abandon rate, or lowering service level, you can set priority promotion to enhance a caller's position in queue. Check the box and enter the proper time interval in seconds.

Supervisor Queue Control

When the **Allow Redirect Call/Change Priority** check box is checked, this allows a workgroup supervisor to redirect queue calls or change the call priority of queued calls, using the MaxSupervisor application.

Queue Management - Advanced

When **Advanced** is selected on the **Queue Management** tab, the **Setup** button becomes available.

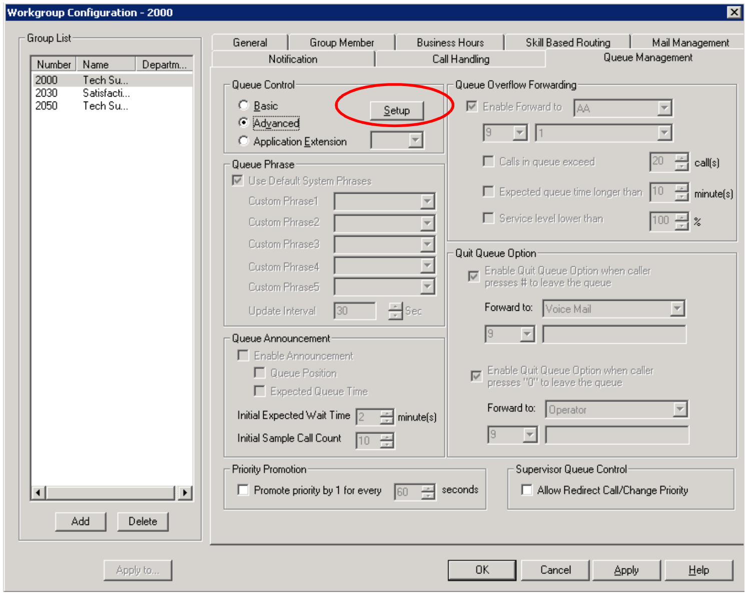


Figure 18-17. Workgroup Configuration, Queue Management, Advanced Queue Control

To configure options for advanced queuing control, click the **Setup** button. This opens the Advanced Queue Management (AQM) application configuration window with tabs for configuring **Announcement**, **Menu Selection**, and **Queue Overflow**.

Announcement

The **Announcement** tab allows for configuration of queue announcements.

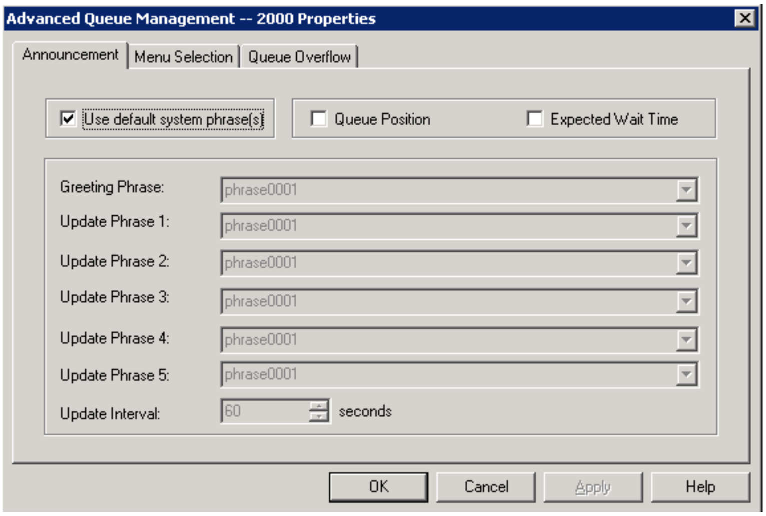

Advanced Queue Management -- 2000 Properties
Announcement
Menu Selection
Queue Overflow
☑ Use default system phrase(s)
□ Queue Position
□ Expected Wait Time
Greeting Phrase: phrase0001
Update Phrase 1: phrase0001
Update Phrase 2: phrase0001
Update Phrase 3: phrase0001
Update Phrase 4: phrase0001
Update Phrase 5: phrase0001
Update Interval: 60 seconds
OK
Cancel
Apply
Help

Figure 18-18. Workgroup Configuration, Advanced Queue Management, Announcement tab

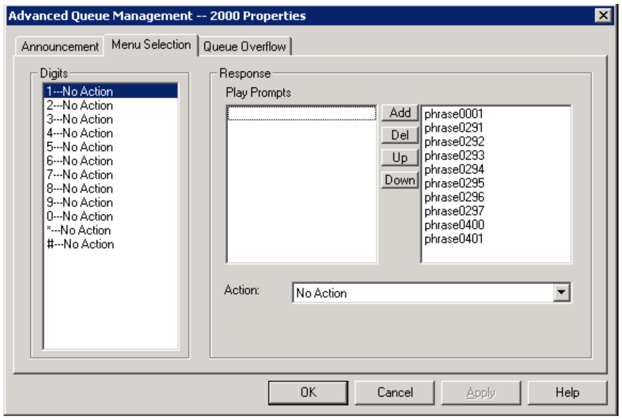
To configure queue announcements:

1. Select any of the following check boxes:
    - **Use Default System Phrases**
    - **Queue Position**
    - **Expected Wait Time**
2. If you are not using default system phrases, use the drop-down lists to select the **Greeting Phrase** and **Update Phrase**s that will be played to callers in queue.
3. Select the **Update Interval** (0 to180 seconds) to be inserted between queue phrases.

    Note: If the interval is set to 0, the system will play phrases one after the other without music in between.
4. Click **OK** or **Apply**.

Menu Selection

The **Menu Selection** tab allows for configuration of a voice menu selection that can be made available to callers in queue. When a workgroup queue is controlled by the Advanced Queue Management application, calls in queue will hear a menu prompt. The menu will allow callers to take certain actions based on digit input, and callers can also hear one or more phrases associated with the actions.



1---No Action
2---No Action
3---No Action
4---No Action
5---No Action
6---No Action
7---No Action
8---No Action
9---No Action
0---No Action
*---No Action
#---No Action

phrase0001
phrase0291
phrase0292
phrase0293
phrase0294
phrase0295
phrase0296
phrase0297
phrase0400
phrase0401

Action: No Action

Figure 18-19. Workgroup Configuration, Advanced Queue Management, Menu Selection tab

To set up the Menu Selection:

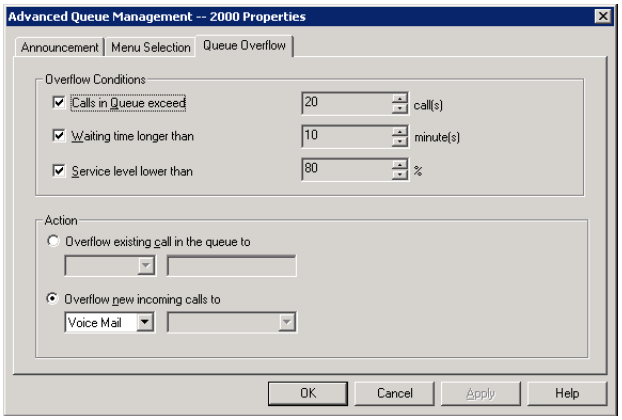
1. In the **Digits** field, select **0** - **9**, **#** or *****.
2. For the highlighted digit, select a **Prompt** from the phrase list and click **Add**. You can add one or more prompts, then use the **Up** or **Down** buttons to determine the order in which the prompts are played.
3. Use the drop-down list to select one of the following actions:
    - **Transfer to Extension/Other Group**
    - **Transfer to AA**
    - **Transfer to Operator**
        - **Transfer to Outside Number**
        - **Transfer to Group VM**
        - **Play prompts**

- **No Action**
- **Disconnect**

4. Click **OK** or **Apply**.

Queue Overflow

The **Queue Overflow** tab allows for configuration of overflow conditions and actions.



Overflow Conditions

☑ Calls in Queue exceed 20 call(s)

☑ Waiting time longer than 10 minute(s)

☑ Service level lower than 80 %

Action

○ Overflow existing call in the queue to

● Overflow new incoming calls to Voice Mail

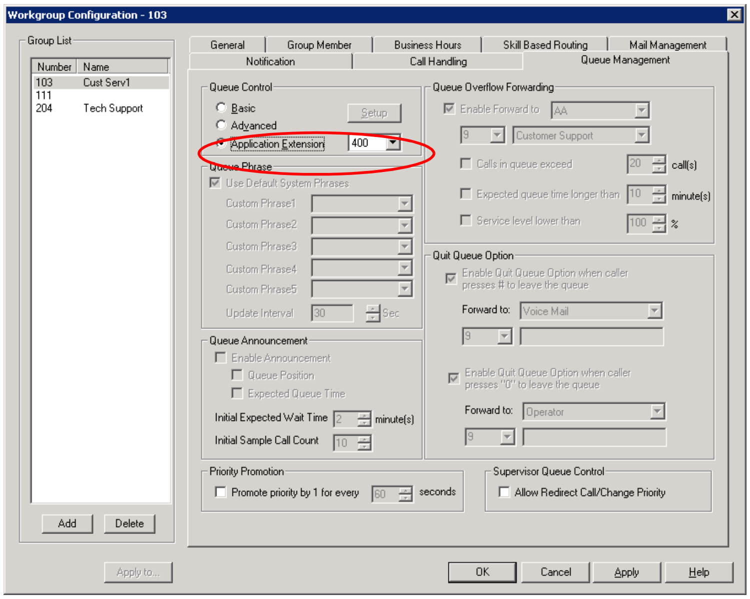
Figure 18-20. Workgroup Configuration, Advanced Queue Management, Queue Overflow tab

- **Overflow Conditions** - select from any of the following check boxes (if all are checked, the conditions will be followed in order):
  - **Calls in Queue exceed** - can be between 0 and 150. This is the number of calls in queue that will cause overflow. For example, 5 calls mean that once a queue has 5 calls in queue, the system will forward the overflow calls according to a specified action.
  - **Wait time longer than** - can be between 0 and 200 minutes. This is the time that a call must have been waiting in queue for the call to be overflowed.
  - **Service level lower than** - can be between 0 and 100%. This is the percentage of calls in queue longer than service level threshold.
- **Action** - select from one of the following options:
  - Overflow existing call in the queue to (first in, first out)
  - Overflow new incoming calls to (last in, first out)

  When either is selected, use the drop-down list to select the overflow action:
  - **Voice Mail**
  - **Extension**—select an extension from the drop-down list.
  - **Workgroup**—select a workgroup from the drop-down list.
  - **AA**—select the auto attendant to use in the drop-down list under the option. AAs are configured in **AA Configuration** on the **System** menu.
  - **Operator**
  - **Outside**—type in the full prefix and phone number, preceded by the trunk or route access code, for example, 915102529712.

Application Extension Queue Control

When you select **Application Extension** in the **Queue Control** panel on the **Queue Management** tab (and an Application Extension is already configured), use the drop-down list to select the desired Application Extension. For more information on configuring an application extension, refer to “Application Extension Configuration” on page 87.



Workgroup Configuration - 103

Group List

Number	Name
103	Cust Serv1
111	
204	Tech Support

Queue Control

○ Basic

○ Advanced

● Application Extension 400

Queue Phrase

☑ Use Default System Phrases

Custom Phrase1

Custom Phrase2

Custom Phrase3

Custom Phrase4

Custom Phrase5

Update Interval 30 Sec

Queue Announcement

□ Enable Announcement

□ Queue Position

□ Expected Queue Time

Initial Expected Wait Time 2 minute(s)

Initial Sample Call Count 10

Queue Overflow Forwarding

☑ Enable Forward to AA

9 Customer Support

□ Calls in queue exceed 20 call(s)

□ Expected queue time longer than 10 minute(s)

□ Service level lower than 100 %

Quit Queue Option

☑ Enable Quit Queue Option when caller presses # to leave the queue

Forward to: Voice Mail

9

☑ Enable Quit Queue Option when caller presses "0" to leave the queue

Forward to: Operator

9

Priority Promotion

□ Promote priority by 1 for every 60 seconds

Supervisor Queue Control

□ Allow Redirect Call/Change Priority

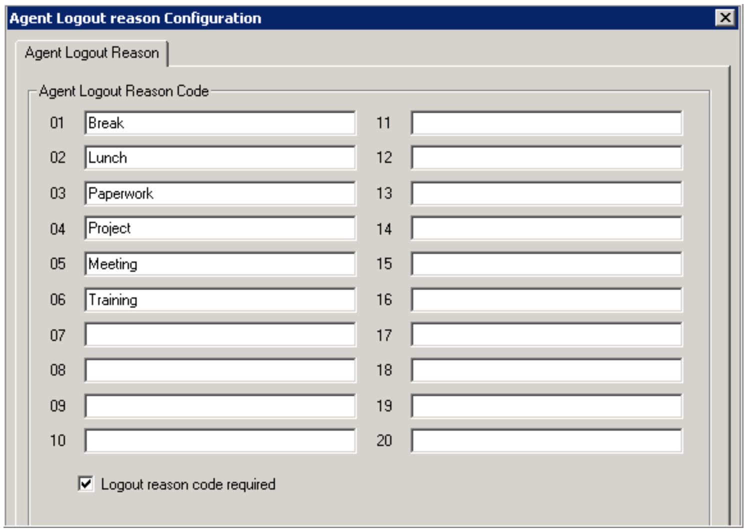
Figure 18-21. Workgroup, Queue Management, Application Extension Queue Control

Agent Logout Reason Codes

In a workgroup environment, logout reason codes allow agents to specify why they are signing off from the workgroup, and the manager can view that information. If logout reasons are required, the system requests a reason at logout from the phone set and from the Agent application.

The **Agent Logout Reason Configuration** window lets you require a logout reason, and it provides for defining up to 20 reason codes. A logout history can be tracked and stored for future analysis.

To access this window, select **CallCenter** > **Agent Logout Reason Configuration**.



01	Break	11	
02	Lunch	12	
03	Paperwork	13	
04	Project	14	
05	Meeting	15	
06	Training	16	
07		17	
08		18	
09		19	
10		20	

☑ Logout reason code required

Figure 18-22. Agent Logout Reason Configuration window

To require logout reasons, check the **Logout reason code required** check box. If you don't want to require reason codes, deselect the check box.

To define reason codes, type the associated reason into the text box next to the code you want to associate with the reason.

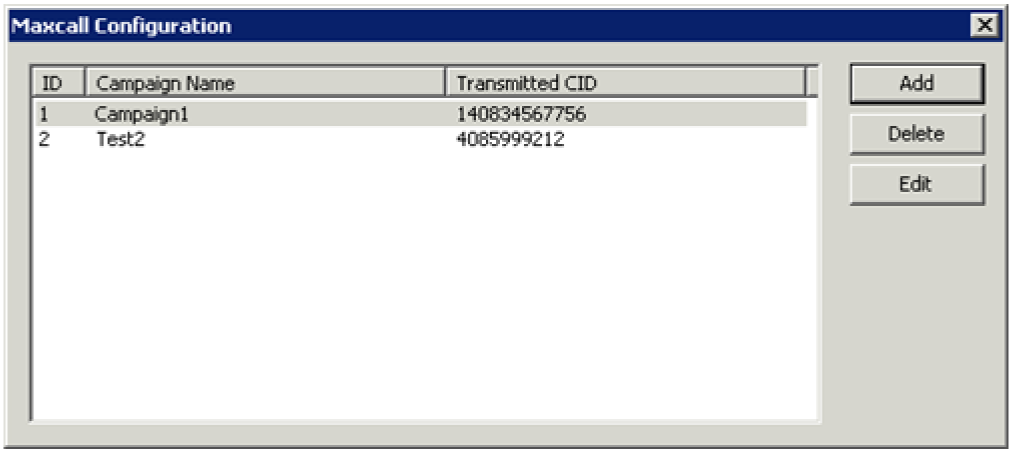
Configuring Workgroup Caller IDs

On the MaxCall tab, you can enter transmitted Workgroup CID numbers for use by agents in the MaxCall application.

Agents can then choose the appropriate CID for each call.

Adding Transmitted CIDs

1. Choose **CallCenter** > **MaxCall Configuration**.
2. Click **Add.**
3. Enter a campaign name and the specific caller ID to transmit when this campaign is chosen by the agent, and then click **OK**.



ID	Campaign Name	Transmitted CID
1	Campaign1	140834567756
2	Test2	4085999212

Figure 18-23. MaxCall caller ID configuration window

Editing Transmitted CIDs

1. Select the campaign that you want to change, and then click **Edit**.
2. Make your changes and click **OK**.

To delete a Transmitted CID, select the campaign and click **Delete**.

CHAPTER

19

Enterprise VoIP Network Management

The VoIP-related aspects of a system are configured in **Enterprise Manager**, available from the **VoIP** menu or the Windows **Start** menu. They include:

- **Codec Profile**—create codec profiles that use different settings for jitter buffer size and packet length. Codec profiles can be assigned to different types of VoIP connections, as defined in the IP dialing table and IP codec assignment table.
- **VoIP Bandwidth Use**—define the maximum VoIP sessions using different codecs on a public Internet or a private intranet data pipe.
- **IP Dialing Table**—define IP dialing digits and codec for VoIP dialing to other MaxACD systems or certified third-party IP devices.
- **IP Codec Table**—define the codec and data pipe for IP devices and SIP trunking service.

Understanding VoIP Bandwidth Requirements

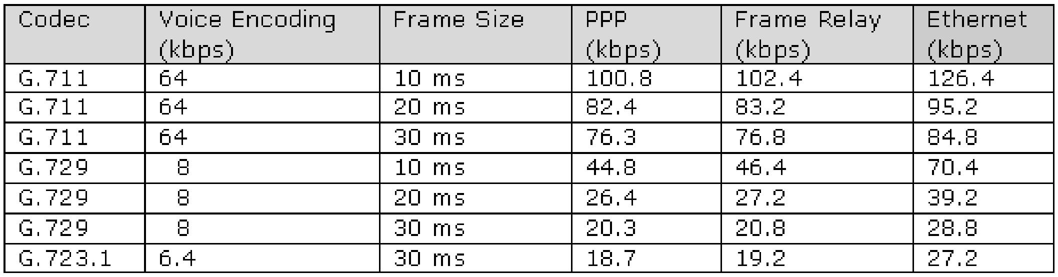
Before starting VoIP-related configurations, it is helpful to have some understanding of VoIP bandwidth requirements, so that you can plan your VoIP deployment properly.

The data network bandwidth required to carry VoIP depends on the following factors:

- **Codec and Compression**—This is the encoding of analog voice to digital form, decoding of digital form to analog wave form, and compression of digital form to a smaller size. MaxACD supports three types of codec: G.711, G.729AB, G.723.1.
- **Packet Length (Frame Size)**—The size of the voice frame data (payload) transmitted in a packet. For G.711 and G.729, you have choice of 10, 20, and 30ms lengths. For G.723.1, the packet length is a fixed 30ms. A larger packet length decreases the transmission overhead. However, it will increase the latency and have a negative effect on the voice quality if a packet is lost during transmission. For G.711 and G.729, 20ms is efficient and recommended.
- **IP Header**—The IP/UDP/RTP header adds 40 octets per packet. With a packet length of 20ms, the IP headers will require 16kbps of bandwidth in addition to whatever codec is being used.
- **Transmission Medium**—In order to travel through the IP network, the IP packet is wrapped in another layer by the physical transmission medium. The transmission medium, such as Ethernet, will add its own header, checksums, and spacers to the packet. With a packet length of 20ms, the transmission medium requires additional 15.2kbps of bandwidth to carry the packets to their destination.

- **Silence Suppression**—You can suppress the transmission of data during periods of silence. This can reduce the demand for bandwidth by as much as 50 percent. However, it may have a negative impact on the voice quality. Some users may feel the conversation is not "natural" when artificial comfort noise is generated during periods of silence.

The following table lists bandwidth requirements for various transmission media with different codecs and frame sizes. It assumes silence suppression is not turned on.



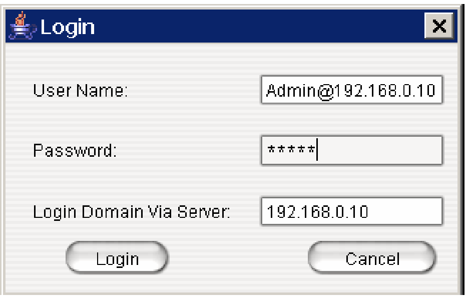
Codec	Voice Encoding (kbps)	Frame Size	PPP (kbps)	Frame Relay (kbps)	Ethernet (kbps)
G.711	64	10 ms	100.8	102.4	126.4
G.711	64	20 ms	82.4	83.2	95.2
G.711	64	30 ms	76.3	76.8	84.8
G.729	8	10 ms	44.8	46.4	70.4
G.729	8	20 ms	26.4	27.2	39.2
G.729	8	30 ms	20.3	20.8	28.8
G.723.1	6.4	30 ms	18.7	19.2	27.2

VoIP Bandwidth requirement for WAN connection varies depending on the type of WAN. Bandwidth requirement typically is less than Ethernet requirement.

Opening Enterprise Manager

To open Enterprise Manager, use one of the following methods:

- From MaxACD Administrator, select **VoIP > Enterprise Network Management**. Enterprise Manager opens without a login dialog box.
- From the Windows **Start** menu, select **All Programs > MaxACD for Lync > Enterprise Manager**. A login screen appears.



User Name: Admin@192.168.0.10

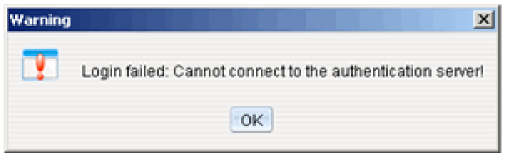
Password: *****

Login Domain Via Server: 192.168.0.10

Figure 19-1. Enterprise Manager login screen

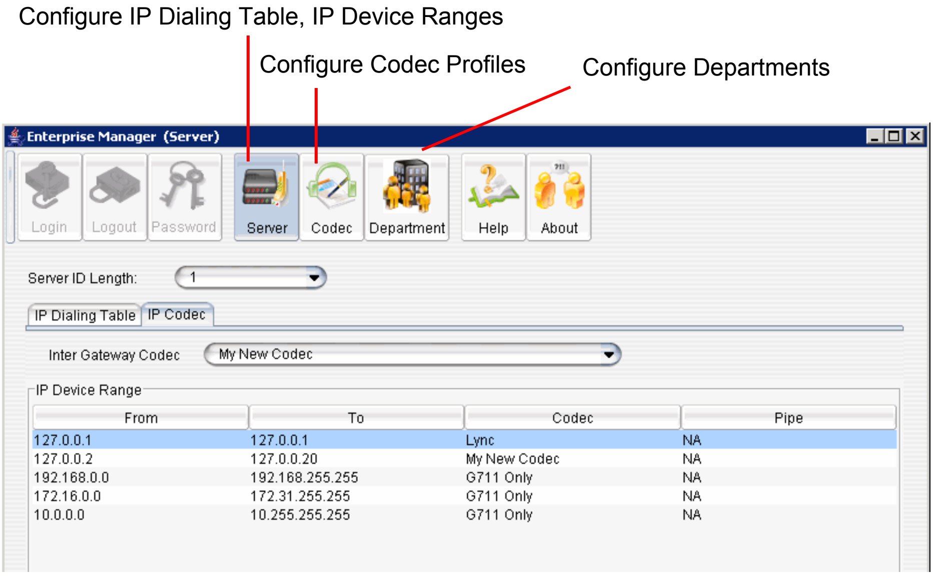
User name	Password	Login Domain Via Server
DomainAdmin (Logging in as **DomainAdmin** gives you rights to change the entire Enterprise Manager configuration.)	Default=22222. You can change the password in Enterprise Manager: Password **Note**: This password is not the same as the MaxACD Administrator password.	Enter the domain master's IP address
Admin@domain master IP address (A Site Admin who logs into the Domain Master in this way has the same rights as DomainAdmin.)	Enter MaxACD Administrator password	Enter the domain master's IP address
Admin@member server IP address (A Site Admin who logs in this way can make changes on this member server only.)	Enter the MaxACD Administrator password for the member server	Enter the member server's IP address

WARNING! If your MaxACD system is using dynamic IP addressing, you will see a warning when opening Enterprise Manager. Please check the Internet Protocol (TCP/IP) Properties of your server NIC interface and assign a fixed IP address to this server.



Login failed: Cannot connect to the authentication server!

Overview of Enterprise Manager



Configure IP Dialing Table, IP Device Ranges

Configure Codec Profiles

Configure Departments

Server ID Length: 1

Inter Gateway Codec: My New Codec

IP Device Range

From	To	Codec	Pipe
127.0.0.1	127.0.0.1	Lync	NA
127.0.0.2	127.0.0.20	My New Codec	NA
192.168.0.0	192.168.255.255	G711 Only	NA
172.16.0.0	172.31.255.255	G711 Only	NA
10.0.0.0	10.255.255.255	G711 Only	NA

Figure 19-2. Enterprise Manager main window

Click a tab to view or configure settings on that tab. Information on a tab is related to the selected server. Click buttons in the toolbar to perform configuration tasks. Click a column heading to sort by that column.

Configuration Buttons

- **Server** button displays the server ID length. On the tabs here you can add and edit IP Dialing Table entries and you can add IP device ranges to a codec.
- **Codec** button lets you configure individual codec profiles—silence suppression, codec, jitter buffer range, RTP packet length, DTMF delivery, enable/disable SIP early media, and SIP transport.
- **Department** button lets you define departments and assign extensions to departments.

Changing the Enterprise Manager Password

Only a person with DomainAdmin rights can change the Enterprise Manager password. To change it, click the **Password** button at the top of the Enterprise Manager window.

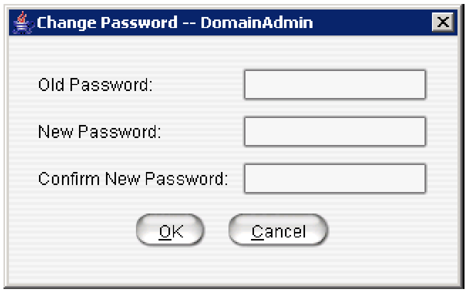


Figure 19-3. Enterprise Manager Log-in dialog box

Enter the old password, and the new password. Confirm the password, and click **OK**.

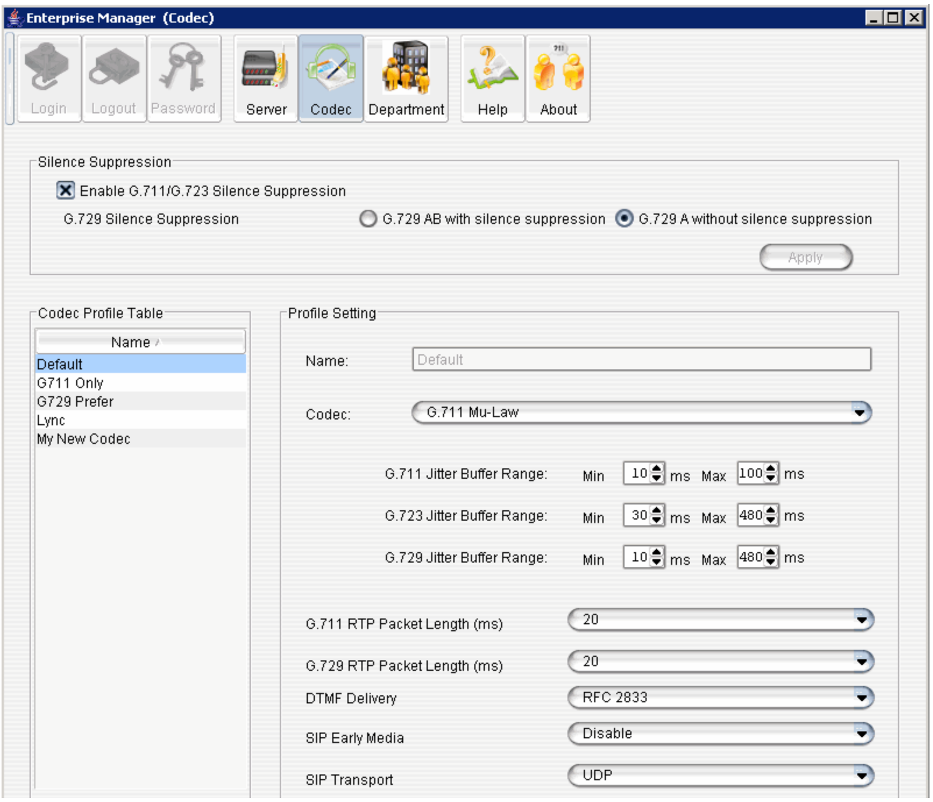
Setting VoIP Codec Profiles

The codec setting is profile-based. For different IP addresses and protocols, a different preferred codec can be used. Each codec profile can have its own codec (G.711, G.723, G.729), packet length, and jitter buffer. The codec profile can be assigned to a VoIP device.

By default, the following IP address ranges (private IP addresses) will use G.711 codec:

- 192.168.0.0 to 192.168.255.255
- 172.16.0.0 to 172.31.255.255
- 10.0.0.0 to 10.255.255.255

To open a window where you can set or modify codec profiles, click the **Codec** button in the Enterprise Manager toolbar.



Silence Suppression

☒ Enable G.711/G.723 Silence Suppression

G.729 Silence Suppression ○ G.729 AB with silence suppression ● G.729 A without silence suppression

Codec Profile Table

Name
Default
G711 Only
G729 Prefer
Lync
My New Codec

Profile Setting

Name: Default

Codec: G.711 Mu-Law

G.711 Jitter Buffer Range: Min 10 ms Max 100 ms

G.723 Jitter Buffer Range: Min 30 ms Max 480 ms

G.729 Jitter Buffer Range: Min 10 ms Max 480 ms

G.711 RTP Packet Length (ms) 20

G.729 RTP Packet Length (ms) 20

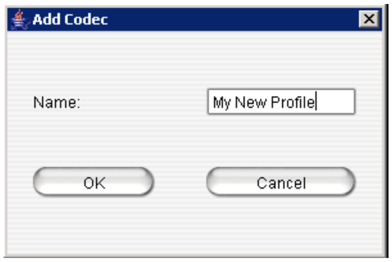
DTMF Delivery RFC 2833

SIP Early Media Disable

SIP Transport UDP

Figure 19-4. Codec profile setting window in Enterprise Manager

Named codec profiles are listed on the left. To create a new profile, click the **Add** button.



Name: My New Profile

Figure 19-5. Add Codec Profile dialog box

Name the new profile, and click **OK**.

Make your changes or additions, and click **Apply**. These are the fields in the Codec configuration window:

Parameter	Description
Codec Profile Table	Lists codec profiles by name. Select a profile in the table to modify its settings, then click **Apply** in the panel where you made the changes. Click the **Add** button to add a codec profile. Click the **Remove** button to remove the selected profile. You cannot remove the Default profile.
Name	Name of the codec profile. You can modify the name, and click **Apply**. The **Default** profile name cannot be changed.
Codec	There are several options: • G.711 Mu-Law • Prefer G.723.1, support G.729 • Prefer G.729, support G.723.1 • G.711 A-Law • Prefer G.711 Mu-Law, support G.711 A-Law • Prefer G.711 A-Law, support G.711 Mu-Law **G.711** provides toll quality digital voice encoding, and **G.723** and **G.729** use low rate audio encoding to provide near toll quality performance under clean channel conditions.
G.711/G.723/G.729 Silence Suppression	When silence suppression is enabled, and silence is detected during a call, MaxACD stops sending packets to the other side. This decreases the bandwidth requirement, however the voice quality may be degraded slightly. These are system-wide settings.
G.711/G.723/G.729 Jitter Buffer Range (ms)	Indicates the delay, in milliseconds, used to buffer G.711/G.723/G.729 voice packets received from the IP network. Voice packets sent over the IP network may incur different delays due to network load or congestion. The jitter buffer helps to smooth out the delay variation in the arriving voice packets and maintain voice quality at the receiving end. The default values for the jitter buffer for G.711 is 10 min. to 100 max milliseconds. The default values for the jitter buffer for G.723 is 30 min. to 480 max milliseconds. The default values for the jitter buffer for G.729 is 10 min. to 480 max milliseconds.
G.711 RTP Packet Length (ms)	Lets you configure the length of the RTP packets for G.711 in milliseconds. The RTP packet length can be set to 10, 20 or 30 milliseconds. The smaller the packet length, the larger the bandwidth required.
G.729 RTP Packet Length (ms)	Lets you configure the length of the RTP packets for G.729 in milliseconds. The RTP packet length can be set to 10, 20 or 30 milliseconds.

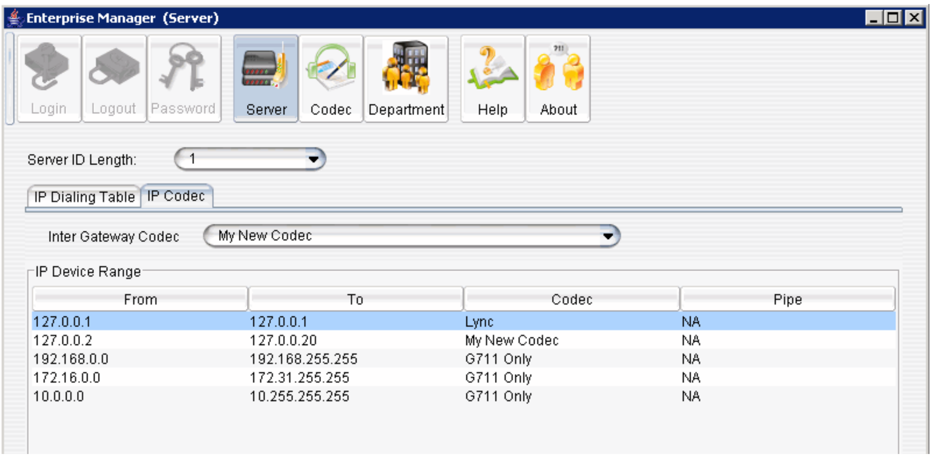
Parameter	Description
DTMF Delivery (Applies to SIP protocol only)	**Default**—If SIP INFO is used to deliver DTMF. **RFC 2833**—The DTMF pay load is embedded with RTP. Most 3rd-party SIP gateways support this standard. **In band**—If DTMF tone is delivered over the voice band. It's not reliable over G.711 codec and will not work over G.729/G.723 codec
SIP Early Media (Applies to SIP protocol and SIP trunk only)	SIP Early Media allows two SIP devices to communicate before a SIP call is actually established. It is important for interoperability with the SIP trunk carrier's PSTN gateway. If **SIP Early Media** is not checked, the caller may not hear the exact ringback tone provided by the CO (the caller may not hear any ringback tone at all).
SIP Transport	There are several SIP Transport options. **UDP**—User Datagram Protocol is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). **TCP**—Transmission Control Protocol is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. **TLS**—Secures SIP signaling messages using Transport Layer Security. **TLS/SRTP**—Adds Secure RTP to Transport Layer Security to secure SIP-associated media. (If this option is chosen, the voice stream always goes through the server.) **Persistent TLS/SRTP**—Persistent TLS/SRTP for SIP signaling messages.

Assigning Codec Profiles to IP Addresses

You can specify what codec profile to use when connecting to VoIP devices.

The codec profile assigned in the IP Device Range table (shown below) supersedes the codec profile defined in the IP dialing table if the IP address is duplicated in both tables.

To set IP address ranges and assign codec profiles to them, in Enterprise Manager click the **IP Codec** tab.



Server ID Length: 1

Inter Gateway Codec: My New Codec

IP Device Range

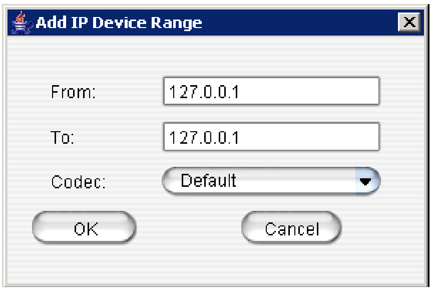
From	To	Codec	Pipe
127.0.0.1	127.0.0.1	Lync	NA
127.0.0.2	127.0.0.20	My New Codec	NA
192.168.0.0	192.168.255.255	G711 Only	NA
172.16.0.0	172.31.255.255	G711 Only	NA
10.0.0.0	10.255.255.255	G711 Only	NA

Figure 19-6. Enterprise Manager IP Codec tab

By default, all private addresses are set to G.711 codec only. You can add individual IP addresses and address ranges and assign a codec to each.

To add IP addresses and address ranges and assign a codec

1. Click the **Add** button in the IP Device Range panel. The Add IP Device Range dialog box opens:



From: 127.0.0.1

To: 127.0.0.1

Codec: Default

Figure 19-7. Add IP Device Range dialog box

2. Enter an IP address range (for dynamic IP addressing), or enter the same address in each field if this is a static address. You cannot use the minimum and maximum values (0.0.0.0. and 255.255.255.255).
3. Click **OK**.

Defining the IP Dialing Table

The IP Dialing Table is used for creating location-based VoIP routing in the enterprise. It supports SIP dual protocol.

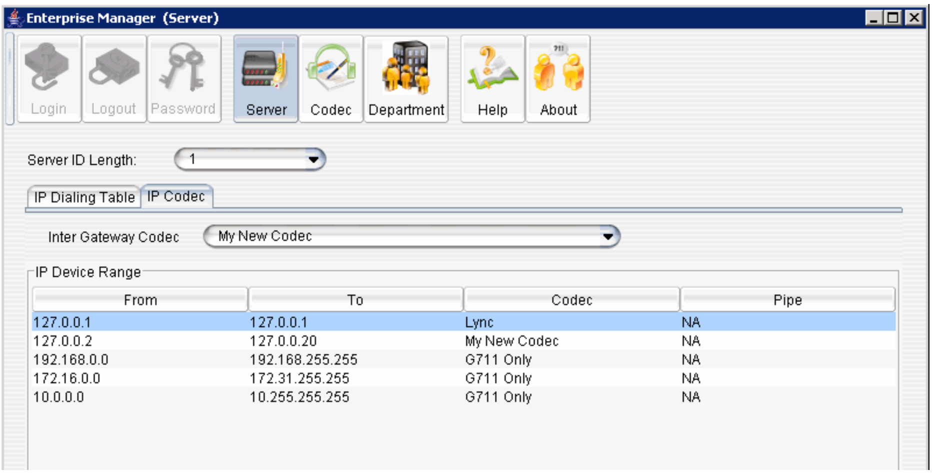
To use a MaxACD-to-MaxACD connection for VoIP, you need to configure the routing in the IP Dialing Table for each MaxACD system.

Notes

- You must assign an IP Trunk Access code (**System Configuration > Number Plan** tab)

- You must set the VoIP codec profiles.

To manage the IP dialing table, click the **IP Dialing Table** tab in Enterprise Manager:



Server ID Length: 1

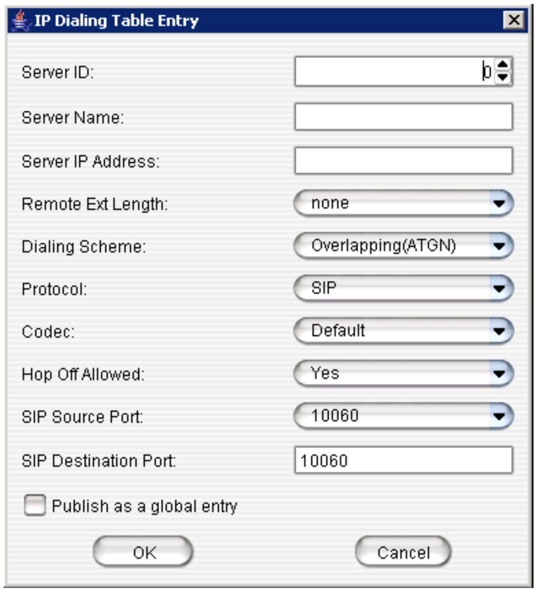
Inter Gateway Codec: My New Codec

IP Device Range

From	To	Codec	Pipe
127.0.0.1	127.0.0.1	Lync	NA
127.0.0.2	127.0.0.20	My New Codec	NA
192.168.0.0	192.168.255.255	G711 Only	NA
172.16.0.0	172.31.255.255	G711 Only	NA
10.0.0.0	10.255.255.255	G711 Only	NA

Figure 19-8. Enterprise Manager IP Dialing Table tab

To add an entry to the IP Dialing Table, click the **Add** button below the table.



Server ID:	0
Server Name:	
Server IP Address:	
Remote Ext Length:	none
Dialing Scheme:	Overlapping(ATGN)
Protocol:	SIP
Codec:	Default
Hop Off Allowed:	Yes
SIP Source Port:	10060
SIP Destination Port:	10060

☐ Publish as a global entry

Figure 19-9. Enterprise Manager IP Dialing table entry dialog box

Define the attributes for the entry:

Parameter	Description
Server ID	A *unique* dialing number to connect to the remote server. The server could be MaxACD, a 3rd-party VoIP gateway, or an AltiGen-certified 3rd-party VoIP device.

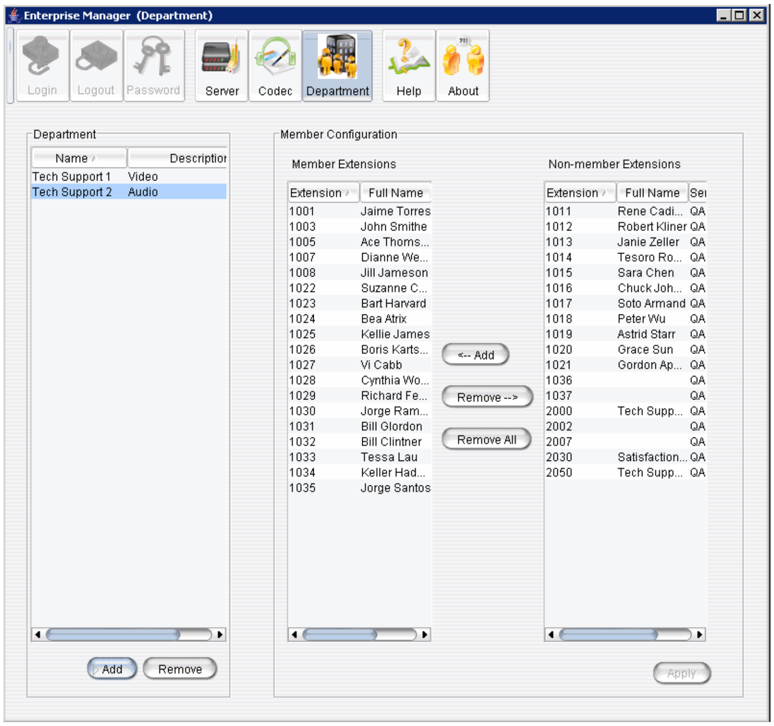
Parameter	Description
Server Name	A descriptive name of up to 15 characters to identify the server. This name may be used by Caller ID.
Server IP Address	The remote server's address. If the server has multiple IP addresses, enter the one that other servers will use to communicate to this system. This IP address format is recommended over DNS names, since with the IP address, the application does not need to resolve the name. DNS name is also posted in this field.
Remote Ext. Length	The length of extension digits at the remote location. Valid entries are None - 7, with "None" meaning not specified. Specifying the remote extension length is optional but highly recommended, since this information tells the system how long to wait for another entry before sending the digits.
Dialing Scheme	**Overlapping (ATGN)** allows the terminal to omit part of the digits required to complete a call while buffering the remaining digits. This results in faster response time, but it only works if the other end is also a MaxACD system. **Enbloc** allows the system to buffer all of the digits required to complete a call.
Protocol	**SIP** Destination supports SIP protocol (selected by default).
Codec	Select which codec profile to use. If the selected profile is incompatible with the remote end, the call will not go through. If you create two items that point to the same IP address, they must also use the same codec. Specifying a different codec is an invalid configuration. MaxACD will always use the codec defined in the first item.
Hop Off Allowed	Choosing **Yes** allows calls from this remote system to hop off to the PSTN by using the trunks in this system. Hop-off capability can be enabled or disabled on a per IP Dialing Table Location basis.
SIP Source Port	Used by UDP only. Choose the SIP source port.
SIP Destination Port	Used by UDP only. Is 10060, by default.

Configuring Departments

Departments can be defined in Enterprise Manager and added to extensions. An extension in one MaxACD system can be assigned to only one department.

In MaxACD Administrator, the department field is displayed on the Extension **General** tab. In MaxACD Agent, the department is displayed on the **Monitor** tab.

To define a department and assign or remove members from a department, click the **Department** button.



Name	Description
Tech Support 1	Video
Tech Support 2	Audio

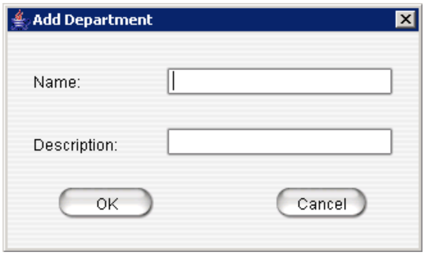
Extension	Full Name
1001	Jaime Torres
1003	John Smithe
1005	Ace Thoms...
1007	Dianne We...
1008	Jill Jameson
1022	Suzanne C...
1023	Bart Harvard
1024	Bea Atrix
1025	Kellie James
1026	Boris Karts...
1027	Vi Cabb
1028	Cynthia Wo...
1029	Richard Fe...
1030	Jorge Ram...
1031	Bill Glordon
1032	Bill Clintner
1033	Tessa Lau
1034	Keller Had...
1035	Jorge Santos

Extension	Full Name	Se
1011	Rene Cadi...	QA
1012	Robert Kliner	QA
1013	Janie Zeller	QA
1014	Tesoro Ro...	QA
1015	Sara Chen	QA
1016	Chuck Joh...	QA
1017	Soto Armand	QA
1018	Peter Wu	QA
1019	Astrid Starr	QA
1020	Grace Sun	QA
1021	Gordon Ap...	QA
1036		QA
1037		QA
2000	Tech Supp...	QA
2002		QA
2007		QA
2030	Satisfaction...	QA
2050	Tech Supp...	QA

Figure 19-10. Enterprise Manager, Department configuration

To define a department

1. Click the **Add** button at the bottom of the Department panel.



Name:

Description:

Figure 19-11. Add Department dialog box

2. Enter a department name and a description, if desired, and click **OK**.

To configure extensions for departments

1. Select a department in the Department list.
2. To add non-member extensions to the department, select the extensions and click **Add**.
3. To delete extensions from the Member Extensions list, select the extensions, and click **Remove**. To remove all member extensions from a department, click **Remove All**.

CHAPTER

20

Redundancy Configuration

MaxACD for Lync provides for system redundancy (a Redundancy license is required).

Two Softswitch servers, primary and secondary, must be configured. When the active server goes down, the standby server takes control. The change is transparent to direct connected calls. (See *Switchover Considerations* on page 200.)

The minimum configuration for system redundancy requires the following components:

- A primary Softswitch server
- A secondary Softswitch server
- A Redundancy moderator
- A Voicemail server, External Logger, and a CDR database.

The next figures show two common configurations.

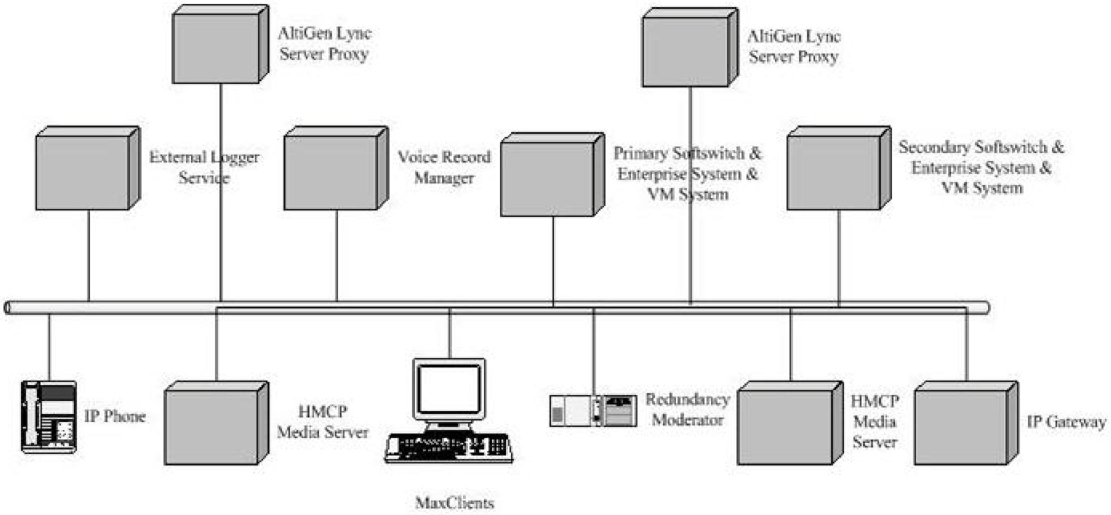

AltiGen Lync Server Proxy
AltiGen Lync Server Proxy
External Logger Service
Voice Record Manager
Primary Softswitch & Enterprise System & VM System
Secondary Softswitch & Enterprise System & VM System
IP Phone
HMCP Media Server
MaxClients
Redundancy Moderator
HMCP Media Server
IP Gateway

Figure 20-1. Redundancy model showing Softswitches on the same LAN

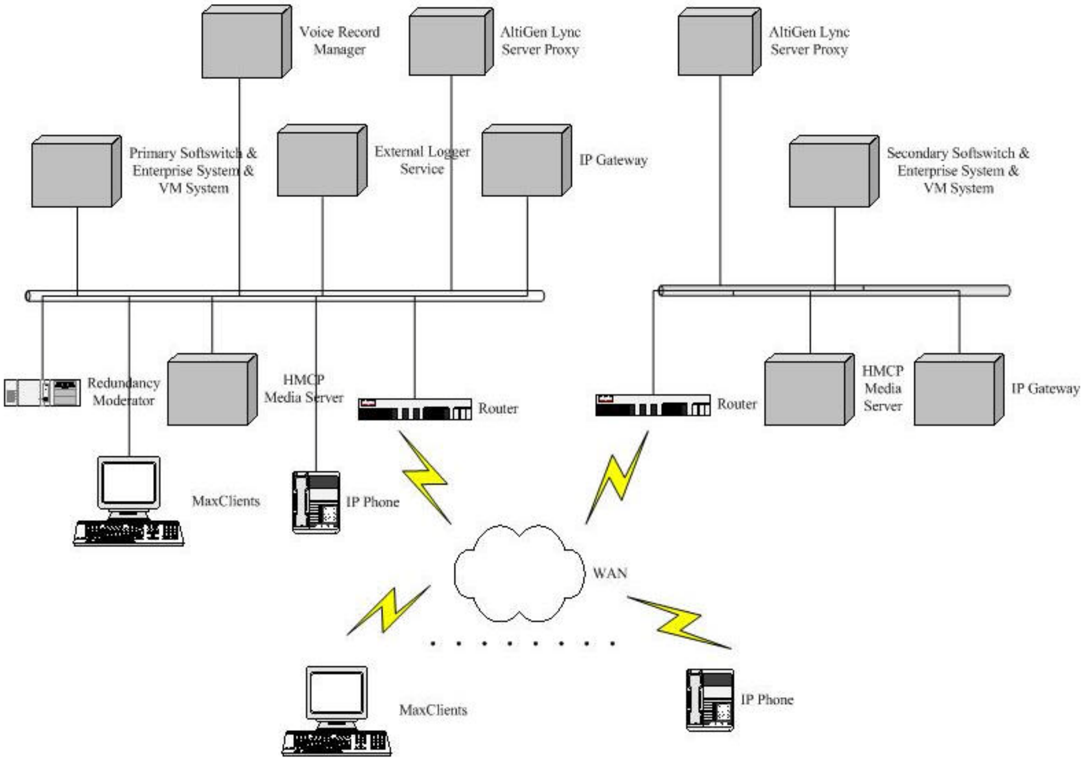


Figure 20-2. Redundancy model showing Softswitches on two different LANs

For scenario two, where the Softswitches are on different LANs, the network between the two LANs must have at least 1Mbps bandwidth and at most 200 ms latency.

Switchover Considerations

Before you implement redundancy, you should understand what happens when the system switches from the active server to the standby server.

In the following cases, MAXCS will switch control of the system from the active server to the standby server:

- When an administrator clicks the **Manual Switch Over** button (see *Manually Switching Servers* on page 208).
- When the active system shuts down or restarts, if the setting **Automatically assume control when active system is not available.** See Figure 20-4, “Redundancy configuration dialog box".
- When the network of the active server disconnects, if the setting **Automatically assume control when active system is not available** is selected.

When system control switches from the active to the standby server, it affects calls in the following ways:

- Current calls will be disconnected. Within a few minutes, new calls will go through.
- CDRs are dropped for all calls, including connected calls.
- Voicemail recording stops.

Requirements

Some system components must be installed on separate servers. This section discusses Voice recording and external applications.

Voice Recording

The target directory of recorded files should be in a server other than the primary and secondary Softswitch.

External Applications

CDR Logger and Database – An External CDR Logger and external CDR database are required in a Redundancy configuration. The active Softswitch will write a CDR to the external logger.

The primary and secondary Softswitches synchronize the next session ID, so that when the secondary Softswitch takes over, its session ID does not duplicate the primary's.

When a Softswitch becomes the active server, it connects with the External CDR Logger. The External CDR Logger drops the original connection when it accepts this new one. The Softswitch has a local buffer where it keeps CDR records when the External Logger connection is unavailable. When the connection with the External CDR Logger is established, these buffered records are written into the external CDR database.

Other Applications – Other applications can be either installed locally on each Softswitch system or run as external applications on a separate machine from the primary and secondary Softswitch. Examples of these external applications include MaxCommunicator, MaxAgent, MaxSupervisor, MaxReports, VRManager, and so on.

All of them have a keep alive connection with the Softswitch. When switchover occurs, each application detects that the connection has broken, and tries to reconnect with the active switching server.

Configuring Redundancy

To set up redundancy, you will follow this general process:

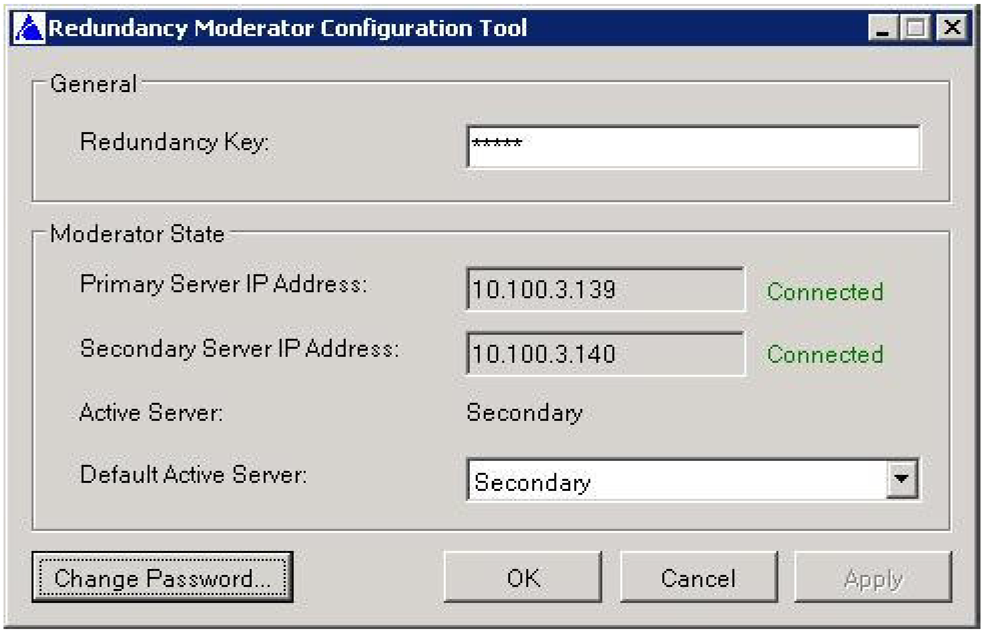
1. Install the Redundancy Moderator; see "Step 1: Install the Redundancy Moderator" on page 202.
2. Configure one server as the primary server; see "Step 2: Configure the Primary Server" on page 203.
3. Configure the other server as the secondary server, adjusting its settings to match those of the primary server. See "Step 3: Configure the Secondary Server" on page 203.
4. Reboot the servers; see "Step 5: Reboot Servers and Restart Services" on page 205.
5. Set the secondary server to take control when appropriate; see "Step 6: Set the Secondary Server to Assume Control" on page 206.
6. Configure the DNS name in your DNS server; see "Step 7: Configure the DNS Name" on page 206.
7. Set up switchover notifications (optional); see "Step 8: Configure Switchover Alerts" on page 207.

Step 1: Install the Redundancy Moderator

We recommend that you install the Redundancy Moderator on the same LAN as the server you will assign as the primary server.

The Redundancy moderator runs as a Windows service.

1. To install the Redundancy Moderator, open the folder *Redundancy Moderator* on the MaxACD installation CD and run *setup.exe* in that folder.
2. After you have installed Redundancy Moderator, you must configure it. Go to the server where you installed the moderator, and in Windows choose **Start** > **All Programs** > **MaxACD Redundancy Moderator** > **Redundancy Moderator Configuration Tool**.
3. Enter the password (the default password is 22222).



Redundancy Moderator Configuration Tool

General

Redundancy Key: *****

Moderator State

Primary Server IP Address: 10.100.3.139 Connected

Secondary Server IP Address: 10.100.3.140 Connected

Active Server: Secondary

Default Active Server: Secondary

Figure 20-3. Redundancy Moderator dialog box

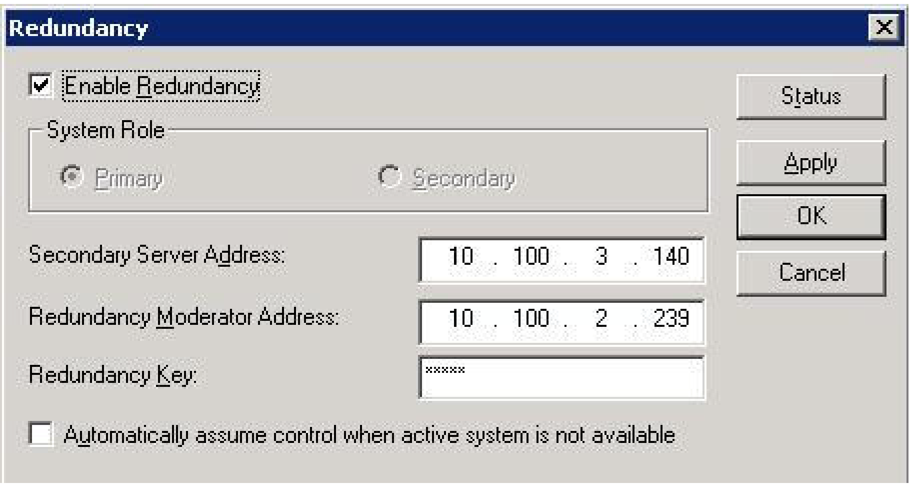
4. Enter a redundancy key. This key is used to authenticate the connection from the primary and secondary Softswitches. You must use the same redundancy key on both the primary and secondary server. The IP addresses of the primary and secondary server will appear, once the servers connect to the moderator.
5. Choose which server you want as the default active server (primary or secondary), and then click OK.
   - If you choose **None**, the moderator service will reject the querying command from the Softswitches.
   - If the states of the two servers ever fall into conflict, the servers will connect to the moderator service and check the **Default Active Server** field to determine which server should be active.
   - When a switchover occurs, the new active server will send a command to the moderator server to update this field.

When you are ready to change the default password, click **Change Password** and specify a new one.

Step 2: Configure the Primary Server

Next you will configure settings in MaxACD Administrator.

1. Log into MaxACD Administrator on the primary server.
2. Install the Redundancy license.
3. On the **System** tab, choose **Redundancy**.



Redundancy

☑ Enable Redundancy

System Role

● Primary ○ Secondary

Secondary Server Address: 10 . 100 . 3 . 140

Redundancy Moderator Address: 10 . 100 . 2 . 239

Redundancy Key: *****

☐ Automatically assume control when active system is not available

Figure 20-4. Redundancy configuration dialog box

4. Check the **Enable Redundancy** check box.
5. Select **Primary** as the system role.
6. Enter the IP addresses for the secondary server and the Redundancy Moderator that you installed in the previous step, and click **OK**.

Step 3: Configure the Secondary Server

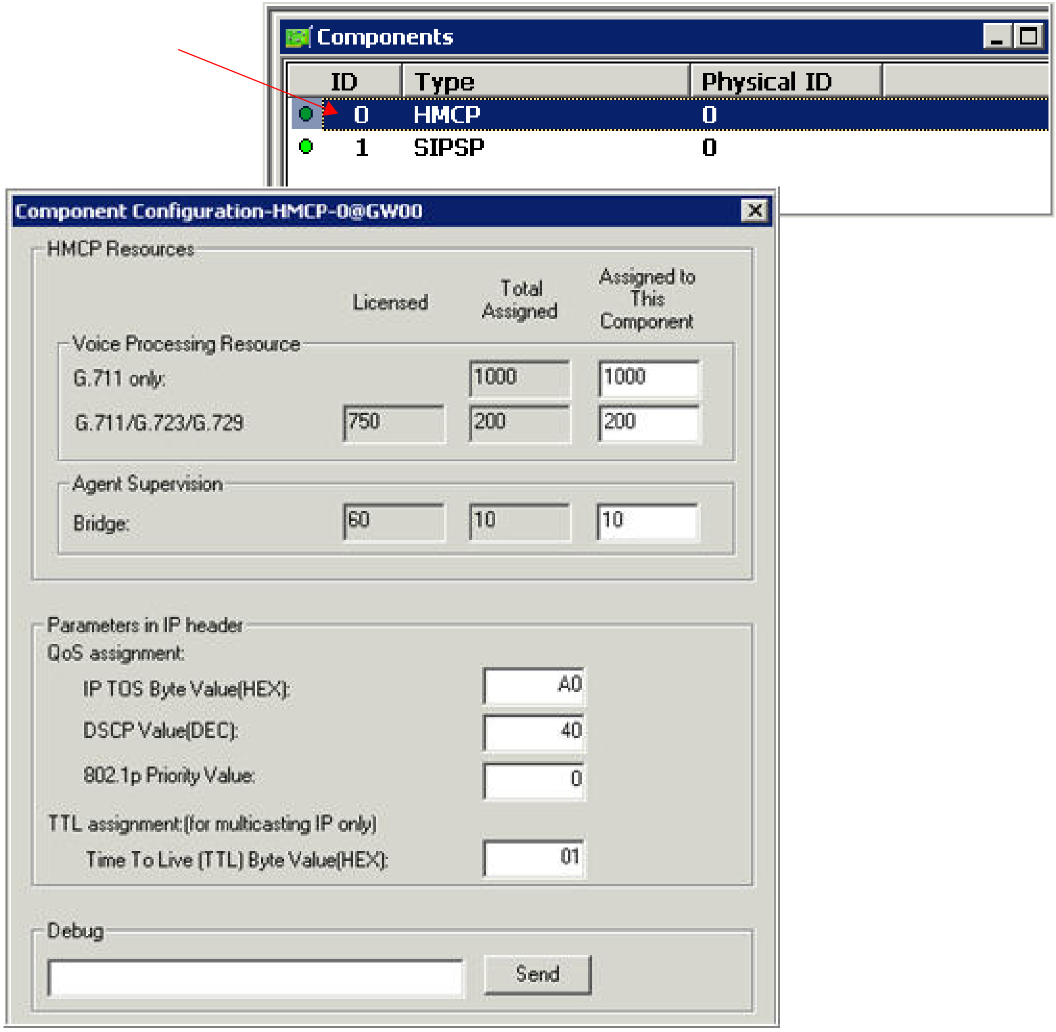
Next, you will configure the secondary server.

1. Log into MaxACD Administrator on the secondary server.
2. On the **System** tab, choose **Redundancy**.
3. Select **Secondary** as the system role.
4. Enter the IP address for the primary server.
5. Enter the redundancy key (it must be the same key as on the primary server) and click **OK**.

Step 4: Copy Settings to Secondary Server

In order for redundancy to work, the secondary server must have *exactly* the same HMCP and SIPSD settings as the primary server.

1. Log into MaxACD on the primary server.
2. In the Components pane, double-click **HMCP** and click **Component Configuration**.



Components

ID	Type	Physical ID
● 0	HMCP	0
● 1	SIPSP	0

Component Configuration-HMCP-0@GW00

HMCP Resources

	Licensed	Total Assigned	Assigned to This Component
Voice Processing Resource			
G.711 only:		1000	1000
G.711/G.723/G.729	750	200	200
Agent Supervision			
Bridge:	60	10	10

Parameters in IP header

QoS assignment:

IP TOS Byte Value(HEX): A0

DSCP Value(DEC): 40

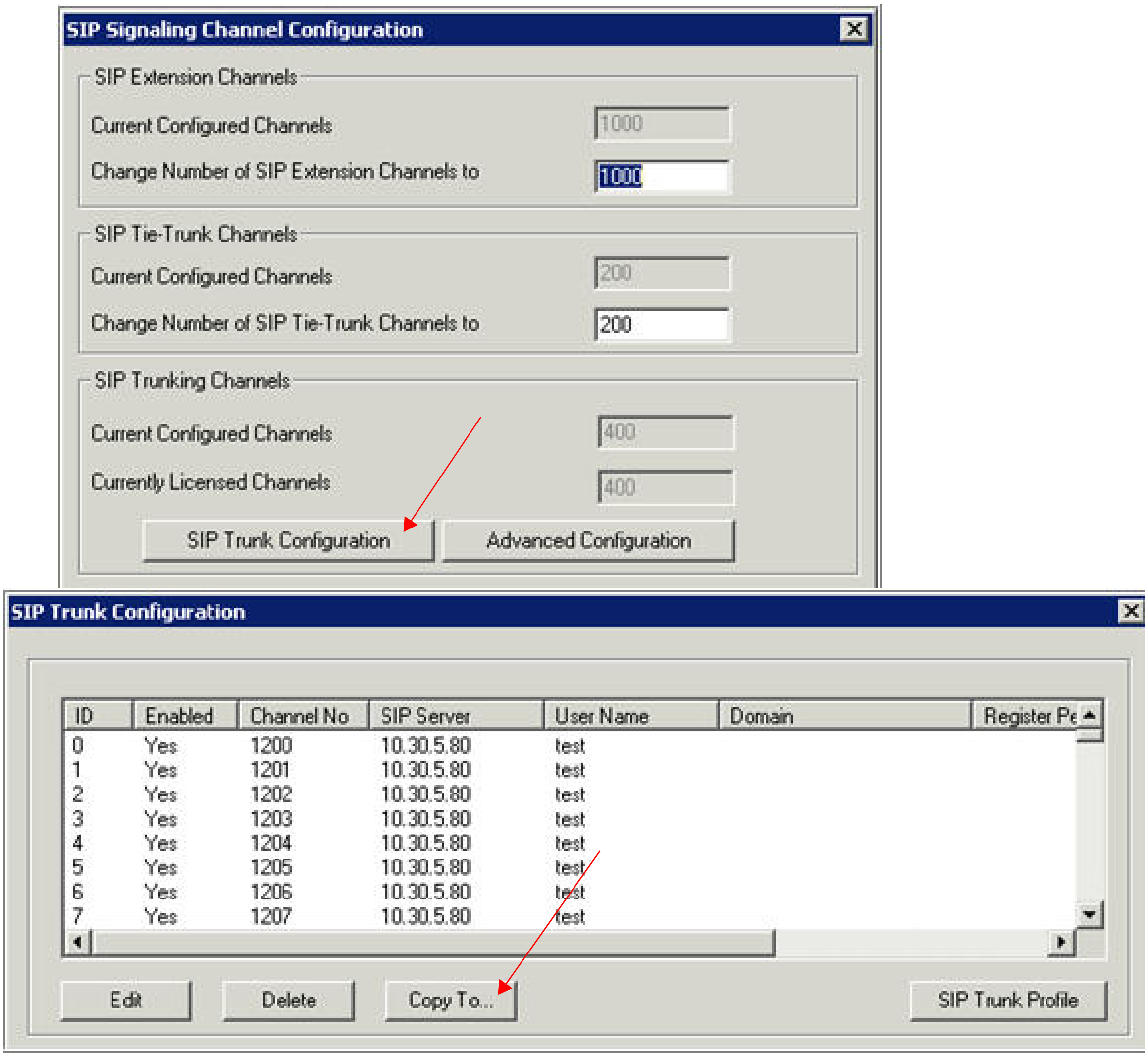
802.1p Priority Value: 0

TTL assignment:(for multicasting IP only)

Time To Live (TTL) Byte Value(HEX): 01

Figure 20-5. HMCP Component configuration dialog box

3. Jot down all of these settings or take a screen capture, so that you can match each setting in the secondary server. Close those dialog boxes.
4. In the Components pane, double-click **SIPSD** and click **Component Configuration**.
5. Jot down all of these settings.
6. Click **SIP Trunk Configuration**. In the dialog box, click **Copy To** and copy those rows to a file. Close those dialog boxes.



SIP Signaling Channel Configuration

SIP Extension Channels

Current Configured Channels: 1000

Change Number of SIP Extension Channels to: 1000

SIP Tie-Trunk Channels

Current Configured Channels: 200

Change Number of SIP Tie-Trunk Channels to: 200

SIP Trunking Channels

Current Configured Channels: 400

Currently Licensed Channels: 400

SIP Trunk Configuration

ID	Enabled	Channel No	SIP Server	User Name	Domain	Register Pe
0	Yes	1200	10.30.5.80	test		
1	Yes	1201	10.30.5.80	test		
2	Yes	1202	10.30.5.80	test		
3	Yes	1203	10.30.5.80	test		
4	Yes	1204	10.30.5.80	test		
5	Yes	1205	10.30.5.80	test		
6	Yes	1206	10.30.5.80	test		
7	Yes	1207	10.30.5.80	test		

Figure 20-6. SIPSD and SIP Trunk dialog boxes

7. Log into MaxACD on the secondary server and replicate all of the settings from the primary server. Open MaxAdministrator and choose **Extension Configuration.**
8. On the **General** tab, choose the number and click the **Apply To** button.

Step 5: Reboot Servers and Restart Services

You must reboot the servers and restart the service before you proceed. You can use the AltiGen *Start & Stop all MaxACD Services* tool for this; see “Start & Stop All MaxACD Services” on page 230.

1. Shut down all services of the secondary server.
2. Shut down all services of the primary server.
3. Restart all services of the primary server.
4. Restart all services of the secondary server.

5. Log onto the Lync Server.
6. Under Voice Routing, choose the **Route** tab and configure the IP addresses of both the primary and secondary server as the PTSN gateway.

Step 6: Set the Secondary Server to Assume Control

1. Log into MaxACD Administrator on the secondary server.
2. On the **System** tab, choose **Redundancy**.
3. Check the option **Automatically assume control when active system is not available**.

Note: This option is only available for the standby server. Once switchover occurs, the formerly active server is now the standby server. This option for the new standby system will be unchecked. You should check it manually after making sure that the new standby system is recovered.

Step 7: Configure the DNS Name

In order for redundancy to work, follow these guidelines:

- You must set up a single DNS name that maps to the two different IP addresses (primary and secondary servers)
- The DNS name must be a new (unused) FQDN
- Clients must refer to the FQDN server pool name, rather than an individual IP address, in order to connect to MaxACD

Important: **Do not use an existing machine name as the DNS name.**

When external services and applications query the DNS name, they will get two IP addresses: the first one is the address of the primary server; the second is the address of secondary server. External services and applications will try to connect to the first IP address. If that connection fails, they will then try to connect to the second IP address. The next connection will always try the address which worked at last login.

The next example will work for MaxACD redundancy:

- *MaxACDSys* with this IP address: 10.30.5.212
- *MaxACDSys* with this IP address: 10.30.5.171

With these settings, all client applications would point to MaxACDSys.domain.com instead of pointing to one IP address.

The next example will not work; redundancy will fail:

- *MaxABC* with this IP address: 10.30.5.212
- *MaxXYZ* with this IP address: 10.30.5.171

You should not create an entry *MaxABC* for 10.30.5.171 in the DNS server and have all clients point to it. If you do, the DNS server will remove the entry automatically and redundancy will fail.

Two FQDN names are also supported: one for the public address and another for the private IP address.

When switchover occurs, external services and applications switch to the other IP address and re-login to new active system if necessary.

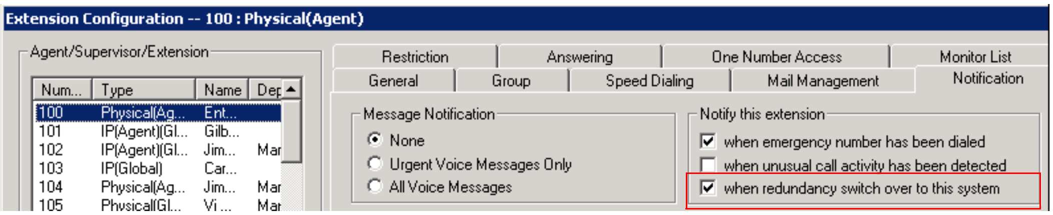
Step 8: Configure Switchover Alerts

While this step is optional, it’s a good practice to have the system send alerts when a switchover occurs.

These alerts take the form off calls, to set extensions, to groups, or to outside numbers.

To configure alerts,

1. Open MaxAdministrator and choose **Extension Configuration.**
2. On the **Notification** tab, select the extension or group number, and check the box **When Redundancy Switch Over to This System**.



Agent/Supervisor/Extension

Num...	Type	Name	Dep
100	Physical(Ag...	Ent...	
101	IP(Agent)(Gl...	Gilb...	
102	IP(Agent)(Gl...	Jim...	Mar
103	IP(Global)	Car...	
104	Physical(Ag...	Jim...	Mar
105	Physical(Gl...	Vi...	Mar

Message Notification

● None
○ Urgent Voice Messages Only
○ All Voice Messages

Notify this extension

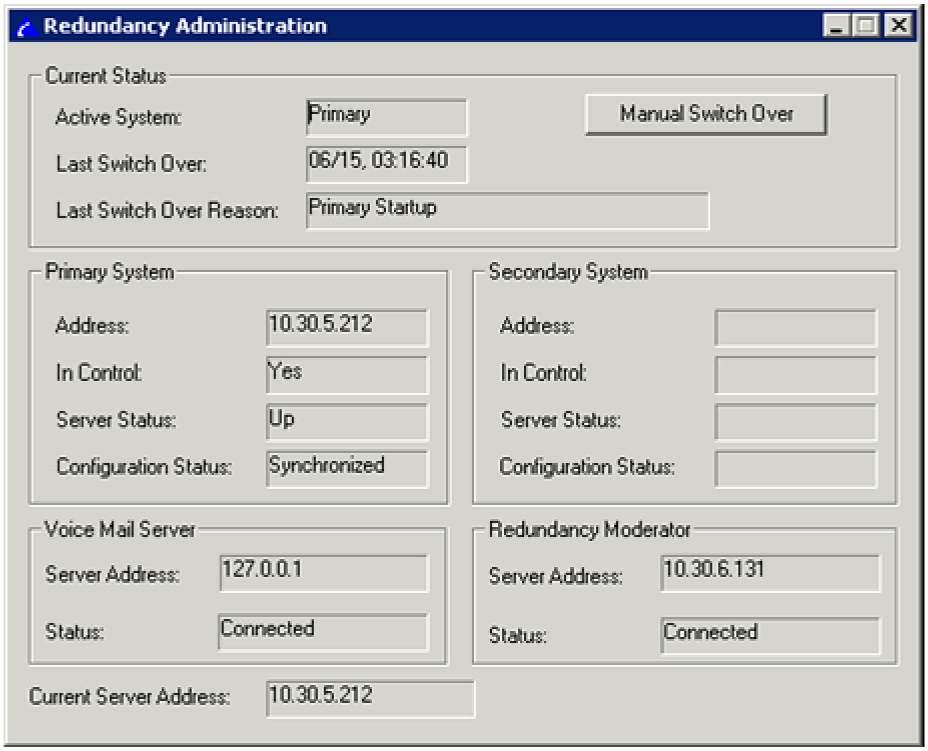
☑ when emergency number has been dialed
☐ when unusual call activity has been detected
☑ when redundancy switch over to this system

Figure 20-7. System Switchover Notification in Extension Configuration

General Maintenance

This section discusses various maintenance tasks that may occur from time to time.

To check redundancy status, from either the primary or secondary server, select **System > Redundancy** and click **Status**.



Current Status

Active System: Primary

Last Switch Over: 06/15, 03:16:40

Last Switch Over Reason: Primary Startup

Primary System		Secondary System	
Address:	10.30.5.212	Address:	
In Control:	Yes	In Control:	
Server Status:	Up	Server Status:	
Configuration Status:	Synchronized	Configuration Status:	

Voice Mail Server		Redundancy Moderator	
Server Address:	127.0.0.1	Server Address:	10.30.6.131
Status:	Connected	Status:	Connected

Current Server Address: 10.30.5.212

Figure 20-8. Redundancy Administration window

Current Status: Shows which server is in control, the date and time of the last switchover, and the reason for the that switchover.

Primary System and **Secondary System**: Shows the status of the two systems. If a server is running, the Server Status field displays *Up*. If a direct service is not detectable, it displays *Down*. You also see the replication status. When replication is complete, the replication status shows *Synchronized*.

Voice Mail Server: Shows the connection status between the active system and the voice mail server (*Connected* or *Disconnected*.)

Redundancy Moderator: Shows the server IP address and the connection status.

A field at the bottom shows the IP address of the active server.

Manually Switching Servers

In the Redundancy Administration window (see Figure 20-8), a **Manual Switch Over** button lets you switch control from the active server to the standby one.

This button is enabled only when all redundancy-related services of both systems are running and the standby server has finished replicating the active server's files.

Rebooting Servers

If you must reboot both systems, or if a SIP-Trunk license is changed, you must reboot both primary and secondary servers to make the changes take effect. The correct order for rebooting is:

1. Shut down the secondary server.
2. Shut down the primary server.
3. Shut down and then restart the Redundancy Moderator.
4. Restart the primary server.
5. Start the secondary server.

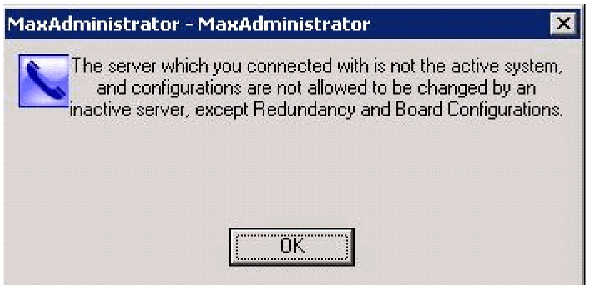
Alternatively, if it’s necessary to shut down both systems, you can disable the “Automatic switch over” feature, and then it doesn't matter in what sequence the systems shut down and boot up. Be sure to enable the automatic switchover feature on the standby system after both servers have restarted.

Updating the Address of the Softswitch Server

If you must change the address of a Softswitch server, you must configure the new address on the VM server and the Enterprise server.

Configure Only on Active System

If you want to configure the system, you must use MaxAdministrator to log onto the active system. If you log on to the inactive system, the following message pops up. Only Redundancy and Board Configuration can be configured on the inactive system.



MaxAdministrator - MaxAdministrator

The server which you connected with is not the active system, and configurations are not allowed to be changed by an inactive server, except Redundancy and Board Configurations.

Figure 20-9. Message from inactive system

Redundancy Limitations

The redundancy feature has the following limitations:

- The Lync client will have a new workgroup login time every time the system switches over.
- Diagnostic trace settings are not synchronized between the primary and secondary servers.
- If the board configuration for the default gateway is changed, or the license for the SIP-Trunk is changed, you must reboot both the primary and secondary systems to make the change take effect. The correct order for reboot is:
  a. Shut down the inactive server.
  b. Shut down the active server, then restart it.
  c. Restart the other server.
- If the active system needs to be shut down for maintenance, control must be manually switched from the active server to the standby server first.

CHAPTER

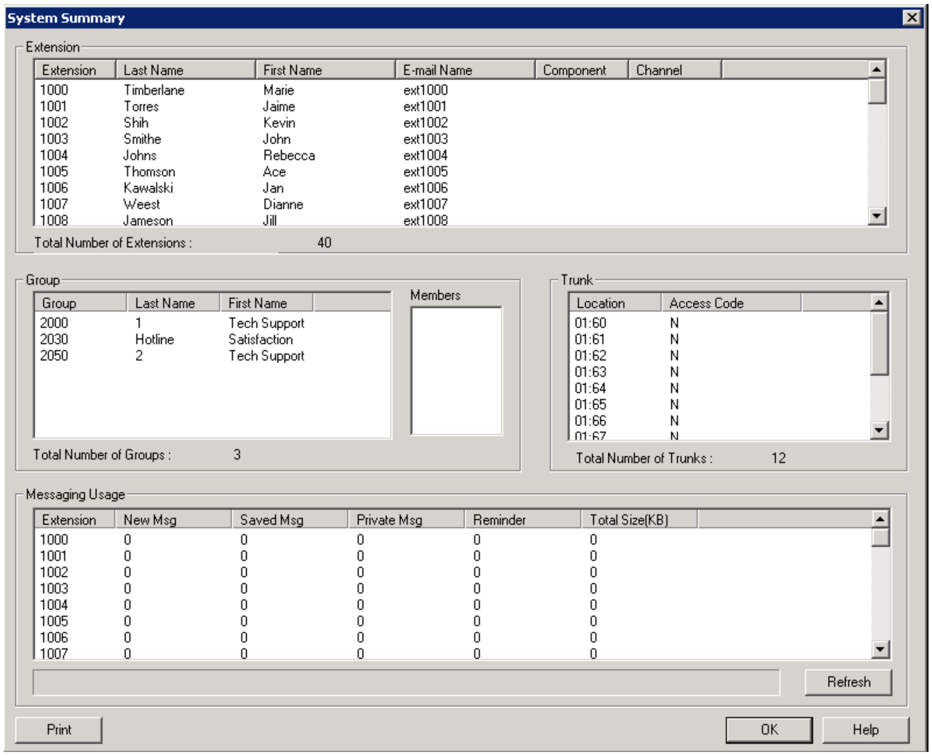
21

System Report Management

MaxACD provides a System Summary report, an IP Cumulative Traffic Statistics report, and an SNMP (Simple Network Management Protocol) configuration screen, all available from the **Report** menu.

System Summary Report

The System Summary report provides summary information on extensions, trunks, and workgroups configured in the system. To open the System Summary report window, select **Report** > **System Summary**, or click the **Summary** button on the toolbar.



System Summary

Extension

Extension	Last Name	First Name	E-mail Name	Component	Channel
1000	Timberlane	Marie	ext1000		
1001	Torres	Jaime	ext1001		
1002	Shih	Kevin	ext1002		
1003	Smithe	John	ext1003		
1004	Johns	Rebecca	ext1004		
1005	Thomson	Ace	ext1005		
1006	Kawalski	Jan	ext1006		
1007	Weest	Dianne	ext1007		
1008	Jameson	Jill	ext1008		

Total Number of Extensions : 40

Group

Group	Last Name	First Name
2000	1	Tech Support
2030	Hotline	Satisfaction
2050	2	Tech Support

Members

Total Number of Groups : 3

Trunk

Location	Access Code
01:60	N
01:61	N
01:62	N
01:63	N
01:64	N
01:65	N
01:66	N
01:67	N

Total Number of Trunks : 12

Messaging Usage

Extension	New Msg	Saved Msg	Private Msg	Reminder	Total Size(KB)
1000	0	0	0	0	0
1001	0	0	0	0	0
1002	0	0	0	0	0
1003	0	0	0	0	0
1004	0	0	0	0	0
1005	0	0	0	0	0
1006	0	0	0	0	0
1007	0	0	0	0	0

Figure 21-1. Reports, System Summary window

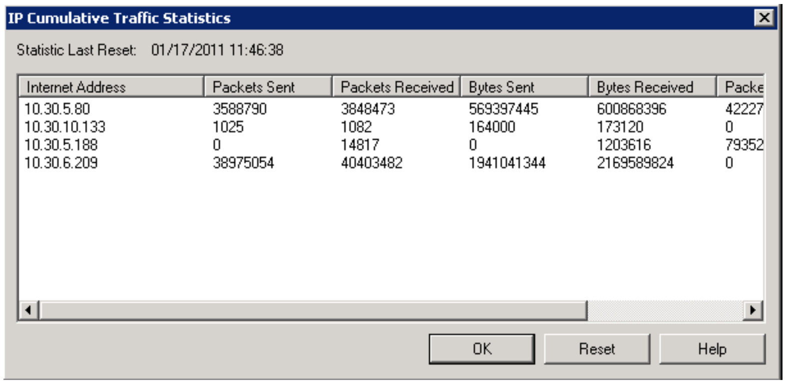
The system summary report displays:

- **Extension Summary**—Configured extensions in the system, including Extension number, Last Name, First Name, SMTP/POP3 E-mail name, Slot (Logical component ID), and Channel.
- **Group Summary**—Configured workgroups in the system. When you select a group, agents belonging to that group are displayed in the Member window.
- **Trunk Summary**—Configured trunks in the system, including trunk location (Component ID : Channel Number) and trunk access code assignment.
- **Messaging Usage**—Message count and storage usage for each mail box. Click the **Refresh** button to update the message count and storage size information.

You can print this report by clicking the **Print** button.

IP Cumulative Traffic Statistics

To view a report of all cumulative IP traffic, click **Reports** > **IP Traffic Statistics**. The window displays IP trunk traffic information for **all** calls:



Statistic Last Reset: 01/17/2011 11:46:38

Internet Address	Packets Sent	Packets Received	Bytes Sent	Bytes Received	Packe
10.30.5.80	3588790	3848473	569397445	600868396	42227
10.30.10.133	1025	1082	164000	173120	0
10.30.5.188	0	14817	0	1203616	79352
10.30.6.209	38975054	40403482	1941041344	2169589824	0

Figure 21-2. Reports, IP Cumulative Traffic Statistics window

This window displays the following data:

Parameter	Description
Internet Address	The IP address of the VoIP system or device.
Packets Sent	Number of voice packets sent to other systems over the public or private IP network.
Packets Received	Number of voice packets received from other systems over the public or private IP network.
Bytes Sent	Total size (in bytes) of all voice packets sent to other systems over the public or private IP network.
Bytes Received	Total size (in bytes) of all voice packets received from other systems over the public or private IP network.
Packets Lost	Number of voice packets that have been lost due to prolonged delays, network congestion, or routing failure.

Parameter	Description
Average Jitter	Average length of delay per voice packet in milliseconds. This figure should stay under 100 milliseconds. A higher figure indicates a longer average delay. This number can be used to measure the quality of service on the network that connects the source and destination sites.

The difference between the **Current Resource Statistics** window and the **IP Cumulative Traffic Statistics** window is that the former shows figures only for the *active* call (Current Traffic) on a particular IP trunk of the local MaxACD system while the other window shows figures for *all* calls combined (cumulative traffic).

Resetting Cumulative Statistics

You can reset the **IP Cumulative Traffic Statistics** by clicking the **Reset** button. Also, this window automatically resets all fields to **0** when the MaxACD system is shut down and restarted. Statistics gathered before the reset are not saved.

Using SNMP

SNMP (Simple Network Management Protocol) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

This MaxACD SNMP configuration, used with a third-party management console (see next section), helps you see the MaxACD status, so you can use MaxACD more securely. Using an SNMPv3 agent, MaxACD sends SNMP traps to the management console when alarming conditions are detected.

Note: The SNMP traps are sent by the MaxACD services SPServ (Softswitch up, Softswitch down traps), AltiKeep (warm start trap), and AltiServ (all other traps), so those services need to be started, or the traps will not be sent.

SNMP Management Console

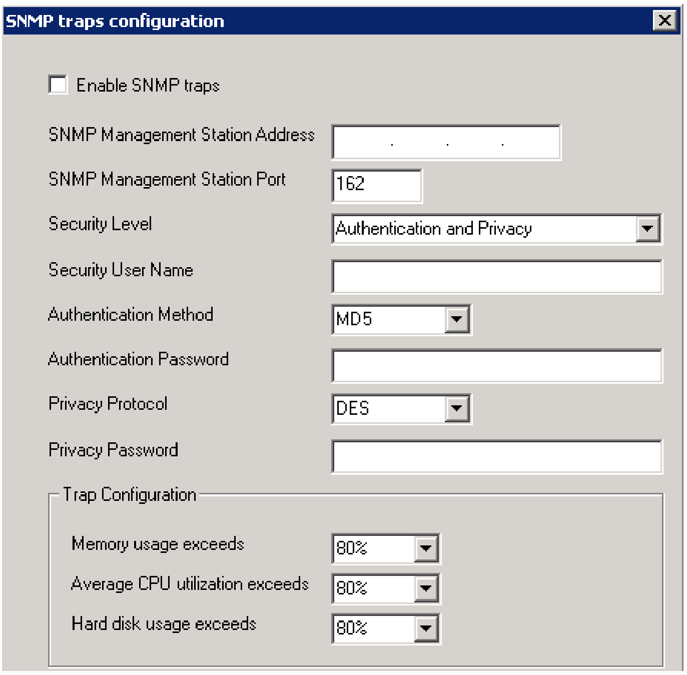
To use SNMP, you need an SNMP management console that is SNMPv3-supported for receiving and collection. If you’re not already using one, AltiGen recommends MG-Soft Trap Ringer Professional Edition, available from MGSoft Corporation, at http://www.mg-soft.com/tringer.html.

You can get help about how to configure an SNMP User Account and Management Console Port in that product’s Help system.

Note: AltiGen’s IANA Private Enterprise Number is 13679.

Configuring MaxACD for SNMP

To configure MaxACD for SNMP, select **Report > SNMP Configuration**.



SNMP traps configuration

☐ Enable SNMP traps

SNMP Management Station Address: . . .

SNMP Management Station Port: 162

Security Level: Authentication and Privacy

Security User Name:

Authentication Method: MD5

Authentication Password:

Privacy Protocol: DES

Privacy Password:

Trap Configuration

Memory usage exceeds: 80%

Average CPU utilization exceeds: 80%

Hard disk usage exceeds: 80%

Figure 21-3. Reports, SMMP Traps Configuration dialog box

Configure the parameters:

- Check **Enable sending SNMP traps**.
- Enter the SNMPv3 server address.
- Enter the SNMPv3 server port.
- Select a security level:
  - No Authentication and No Privacy
  - With Authentication but No Privacy
  - With Authentication and Privacy
- Select an Authentication Method, and enter a password
- Select a Privacy Protocol, and enter a password.
- Configure traps:
  - **Memory usage exceeds** This trap is sent when MaxACD detects that the lowest virtual memory usage exceeds a specified percentage of physical memory configuration within a 10-minute duration. Default value is 80%. The next trap will be sent after the condition is cleared then occurs again. The minimum duration between any two consecutive traps is 30 minutes
  - **Average CPU utilization exceeds** This trap is sent when MaxACD detects its average CPU utilization exceeds a specified percentage in any 10-minute duration. Default value is 80%. The next trap will be sent after the condition is cleared then occurs again. The minimum duration between any two consecutive traps is 30 minutes

- **Hard disk usage exceeds** This trap is sent when hard disk usage of MaxACD transitioning from below threshold to on or above threshold is detected. Default value is 80%. The minimum duration between any two consecutive traps is 30 minutes.

List of Traps Sent

A trap is sent when the following conditions are detected.

- Cold Start (generic trap). When AltiServ is cold started and initialized successfully.
- Warm Start (generic trap). When AltiKeep service detects AltiServ.exe is down, re-starting AltiServ.exe, and AltiServ is initialized successfully.
- LinkDown (generic trap). When detecting a T1/E1/PRI span state is transitioning from up to down or losing clock source.

  When a gateway is down, one trap is sent for each T1/E1/PRI interface in this Gateway. This trap is sent when SIP trunk destination state transitioning from reachable to unreachable is detected.

  Every T1/E1/PRI span and SIP trunk channel is assigned a unique "ifIndex" value as a port identifier
- LinkUp (generic trap). When a T1/E1/PRI span state transitioning from down to up is detected.
- Softswitch up (specific trap). When AltiServ.exe starts to respond to the keep alive packets sent by the SNMP Agent. AltiServ should respond to the keep-alive packets after its initialization is completed.
- Softswitch down (specific trap). When AltiServ.exe stops responding to the keep-alive packets sent by the SNMP Agent.
- Gateway/Media Server connection up (specific trap). When a gateway or HMCP Media Server connection state transitioning from down to up is detected.
- Gateway/Media Server connection down (specific trap). When a gateway or HMCP Media Server connection state transitioning from up to down is detected.
- Enterprise Manager Master up (specific trap). When MaxACD is in Enterprise Manager slave role and Enterprise Manager master state transitioning from down to up is detected.
- Enterprise Manager Master down (specific trap). When MaxACD is in Enterprise Manager slave role and Enterprise Manager master state transitioning from up to down is detected.
- Enterprise Manager Slave up (specific trap). When MaxACD is in Enterprise Manager master role and detects Enterprise Manager slave state transitioning from down to up.
- Enterprise Manager Slave down (specific trap). When MaxACD is in Enterprise Manager master role and detects Enterprise Manager slave state transitioning from up to down.
- IP Phone service up (specific trap). When detecting IP Phone service transitioning from down to up.
- IP Phone service down (specific trap). When detecting IP Phone service transitioning from up to down.
- VM server connection up (specific trap). When detecting VM server connection transitioning from down to up.

- VM server connection down (specific trap). When detecting VM server connection transitioning from up to down.
- CT Proxy Service up (specific trap). When CTProxy Service connection transitioning from down to up is detected.
- CT Proxy Service down (specific trap). When detecting CTProxy Service connection transitioning from up to down.
- Excessive memory usage on Softswitch (specific trap). When MaxACD detects the lowest virtual memory usage exceeds a specified percentage of physical memory configuration within a 10-minute duration. The next trap will be sent after the condition is cleared then occurs again. The minimum duration between any two consecutive traps is 30 minutes.
- Excessive CPU utilization on Softswitch (specific trap). When MaxACD detects its average CPU utilization exceeds a specified percentage in any 10-minute duration. The next trap will be sent after the condition is cleared then occurs again. The minimum duration between any two consecutive traps is 30 minutes.
- Excessive hard disk usage on Softswitch (specific trap). When hard disk usage of MaxACD transitioning from below threshold to on or above threshold is detected. The minimum duration between any two consecutive traps is 30 minutes.
- Redundancy switch-over (specific trap). When a redundancy switch-over between Primary and Secondary Softswitch is detected. This trap is reported by the newly activated Softswitch.

CHAPTER

22

Microsoft Exchange Integration

This chapter provides step-by-step instructions for configuring Microsoft Exchange and MaxACD to work together. Exchange integration synchronizes voice messages between the AltiGen voice mailbox and Exchange mailbox.

Note: An AltiGen Exchange Integration license is required for each extension using Exchange integration.

Requirements

Make sure the following items are ready before Exchange integration is configured. Note that AltiGen is not responsible for, and cannot support, installation of Microsoft Exchange Server:

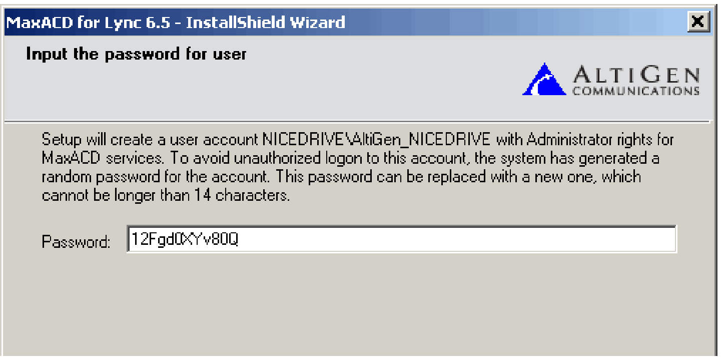
To set up any kind of Exchange integration, you must log in as the Domain Administrator, NOT the Local Administrator. You need the following:

- One Windows server for MaxACD, loaded with:
  - Windows 2003 Server or Windows 2008
  - MaxACD for Lync software
  - Microsoft Outlook client: either Outlook 2007 or Outlook 2010. To integrate with Exchange 2007, Outlook 2007 should be installed at the MaxACD system.
- A *second* Windows server for Exchange, loaded with Exchange Server 2003 or 2007 software, as appropriate. If it is an Exchange 2007 server, it should be installed on 64-bit system(s) with Windows 2003 64-bit or above OS. Unified Messaging, Client Access, and Mailbox Server roles should be installed with Exchange Server 2007.
- The MaxACD system and the Exchange Server system must belong to the *same* domain, with a network throughput rate of no less than 100Mbps and without any Web proxies in between.
- MaxACD Services must be installed and started with the user account <*Domainname*>\AltiGen_<AltiServ*SystemName*>.
- This service account must have a mailbox in the Exchange Server that is different from the previous version.
- Exchange Server Services must be started.
- Successful ping from Exchange Server to MaxACD and *vice versa.*

When You Install MaxACD

You may be installing MaxACD now, or you may have already installed it.

1. If you are installing now, log in to Windows with a user account that is a member of the Domain Admin group. If MaxACD is already installed, skip to step 4.
2. While installing, MaxACD automatically creates a user account as a service account (see Figure 22-1, "MaxACD installation program, user account "AltiGen_NICEDRIVE""), and you can change the default password. Record this password for future troubleshooting.


MaxACD for Lync 6.5 - InstallShield Wizard
Input the password for user
ALTIGEN COMMUNICATIONS

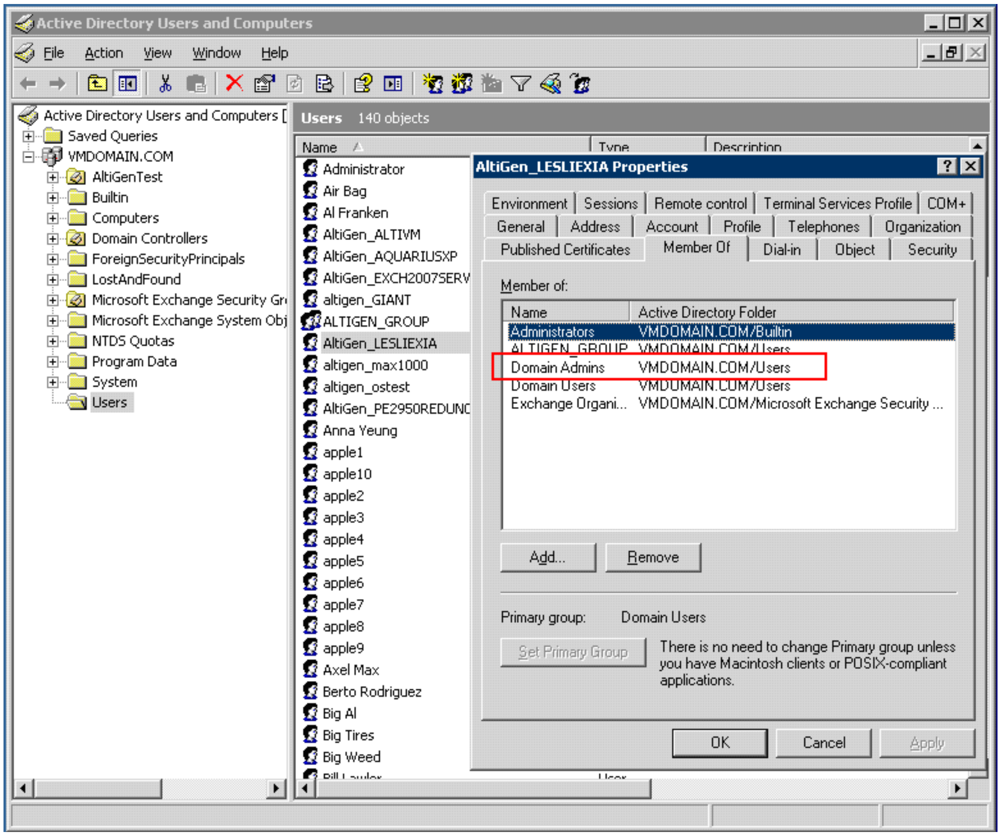
Setup will create a user account NICEDRIVE\AltiGen_NICEDRIVE with Administrator rights for MaxACD services. To avoid unauthorized logon to this account, the system has generated a random password for the account. This password can be replaced with a new one, which cannot be longer than 14 characters.

Password: 12Fgd0XYv80Q

Figure 22-1. MaxACD installation program, user account "AltiGen_NICEDRIVE"

3. After installation, add this user account to the Domain Admin group via Active Directory Users and Computers (see Figure 22-2).
4. If MaxACD was already installed on the system, do the following:
   a. Create a new domain user account, and add it to the Domain Admin group via Active Directory Users and Computers.
   b. Move the MaxACD server to the Domain.
   c. Use the AltiPassword change utility (C:\AltiServ\Exe\AltiPwdChange.exe) to change all MaxACD service accounts to run as this new user account.

Note: In the future, if you need to debug you must log in to the MaxACD server with this user account.



Member of:

Name	Active Directory Folder
Administrators	VMDOMAIN.COM/Builtin
ALTIGEN_GROUP	VMDOMAIN.COM/Users
Domain Admins	VMDOMAIN.COM/Users
Domain Users	VMDOMAIN.COM/Users
Exchange Organi...	VMDOMAIN.COM/Microsoft Exchange Security ...

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

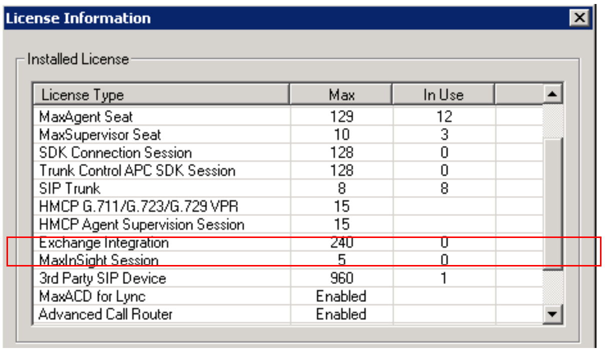
Figure 22-2. MaxACD Active Directory

5. Add the user created by the MaxACD install program (or created by you in step 4) to the Domain Admin group in Active Directory Users and Computers.

Exchange Integration Configuration Steps

After installation, perform the following steps:

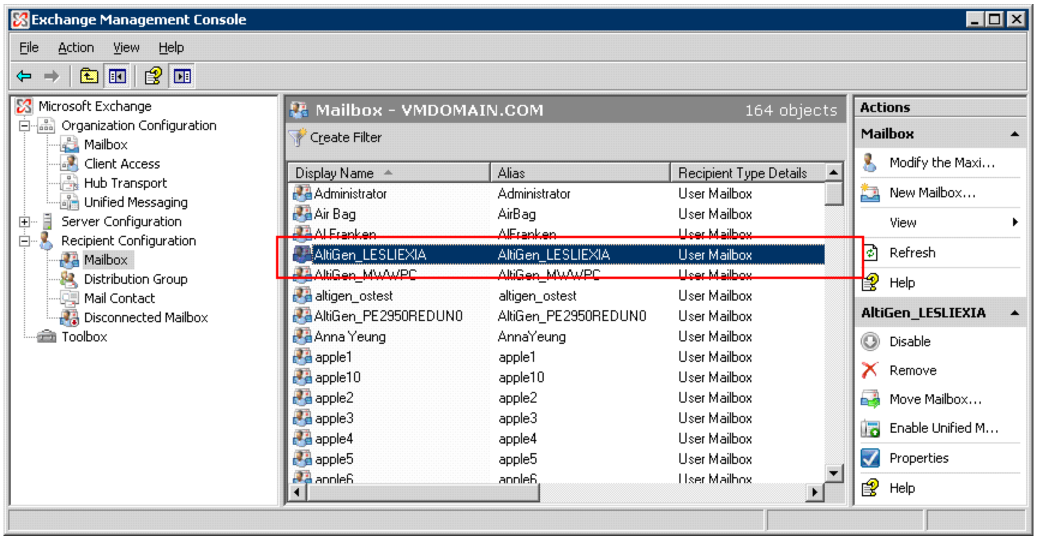
1. Add Exchange Integration licenses to MaxACD; see Figure 22-3.



License Type	Max	In Use
MaxAgent Seat	129	12
MaxSupervisor Seat	10	3
SDK Connection Session	128	0
Trunk Control APC SDK Session	128	0
SIP Trunk	8	8
HMCP G.711/G.723/G.729 VPR	15	
HMCP Agent Supervision Session	15	
Exchange Integration	240	0
MaxInSight Session	5	0
3rd Party SIP Device	960	1
MaxACD for Lync	Enabled	
Advanced Call Router	Enabled	

Figure 22-3. Add Exchange Integration licenses

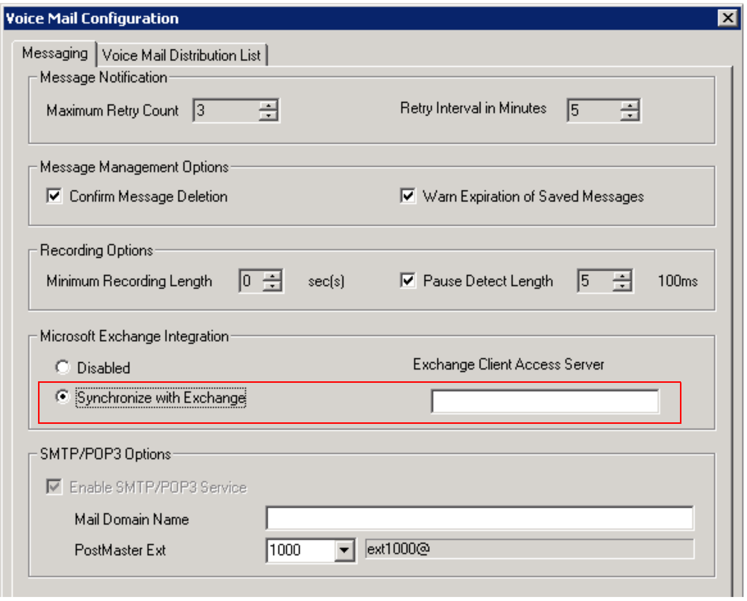
2. In the Exchange Management Console, create a mailbox for the service account that was created during installation (or created by you in step 4, above); see Figure 22-4.



Display Name	Alias	Recipient Type Details
Administrator	Administrator	User Mailbox
Air Bag	AirBag	User Mailbox
Al Franken	AlFranken	User Mailbox
AltiGen_LESLIEXIA	AltiGen_LESLIEXIA	User Mailbox
AltiGen_MWWPC	AltiGen_MWWPC	User Mailbox
altigen_ostest	altigen_ostest	User Mailbox
AltiGen_PE2950REDUN0	AltiGen_PE2950REDUN0	User Mailbox
Anna Yeung	AnnaYeung	User Mailbox
apple1	apple1	User Mailbox
apple10	apple10	User Mailbox
apple2	apple2	User Mailbox
apple3	apple3	User Mailbox
apple4	apple4	User Mailbox
apple5	apple5	User Mailbox
apple6	apple6	User Mailbox

Figure 22-4. Creating a mailbox for the service account created during installation

3. In MaxACD Administrator, choose **System > Voice Mail Configuration**, then select **Synchronize with Exchange**, and enter the name (*not* the IP address) of Exchange server (see Figure 22-5).



Message Notification

Maximum Retry Count 3 | Retry Interval in Minutes 5

Message Management Options

☑ Confirm Message Deletion | ☑ Warn Expiration of Saved Messages

Recording Options

Minimum Recording Length 0 sec(s) | ☑ Pause Detect Length 5 100ms

Microsoft Exchange Integration

○ Disabled

● Synchronize with Exchange | Exchange Client Access Server

SMTP/POP3 Options

☑ Enable SMTP/POP3 Service

Mail Domain Name

PostMaster Ext 1000 ext1000@

Select **Synchronize with Exchange**.

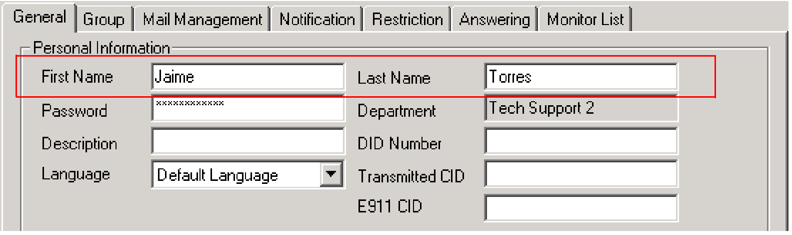
Enter the NAME (*not* the IP address) of the Exchange Server

Figure 22-5. Selecting **Synchronize with Exchange** in MaxACD

4. Configure the names of each extension user such that the first and last names are the same as the user’s matching mailbox on the Exchange Server.

Note: The **Middle Initial** field should be *empty* for Exchange Server mail accounts in order for Exchange integration to work properly.

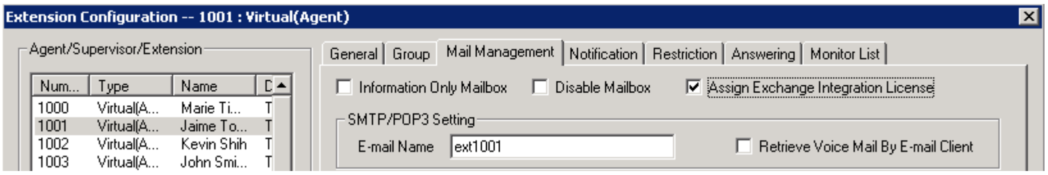
5. MaxACD matches the mailbox on the Exchange Server via the display name, which is a combination of “FirstName LastName”. In the example in Figure 22-6, the display name is “Jaime Torres”, so you should make sure the user’s display name on the Exchange Server is “Jaime Torres”, or synchronization will fail.



First Name: Jaime
Last Name: Torres
Password: ************
Department: Tech Support 2
Description:
DID Number:
Language: Default Language
Transmitted CID:
E911 CID:

Figure 22-6. First and last name in MaxACD

6. For users whose voice mails will be integrated with Exchange, check **Assign Exchange Integration License** on the Extension Configuration screen’s **Mail Management** tab (see Figure 22-7). Make sure that the **E-mail Name** field contains alphanumeric characters only and does not contain other characters such as spaces ( ) or periods (.).



Extension Configuration -- 1001 : Virtual(Agent)

Agent/Supervisor/Extension

Num...	Type	Name	D
1000	Virtual(A...	Marie Ti...	T
1001	Virtual(A...	Jaime To...	T
1002	Virtual(A...	Kevin Shih	T
1003	Virtual(A...	John Smi...	T

☐ Information Only Mailbox ☐ Disable Mailbox ☑ Assign Exchange Integration License

E-mail Name: ext1001 ☐ Retrieve Voice Mail By E-mail Client

Figure 22-7. Assigning the Exchange Integration license to a user

Note: Each user needs to access their mailbox once via Outlook before synchronization will start working for that user.

If necessary, see “Testing for Synchronization” on page 221 and “Troubleshooting Tips” on page 222.

When You Create a New Mailbox User

When you create a new mailbox user in Exchange Server and a new extension in MaxACD, to associate them you need to restart the AltiGen VM Exchange Integration Service.

Testing for Synchronization

You can use some simple procedures to make sure that the **Synchronize with Exchange** integration is working correctly.

To test the integration, set up an extension in MaxACD (for example, extension 1000) and its corresponding mailbox in Exchange Server. Also, set up a PC with Outlook 2007/2010 configured for this user.

To Test Message Delivery to Exchange

1. Leave a voice mail for extension 1000. The message light illuminates.
2. Log on to the Exchange Mailbox from Outlook and check for the message in the inbox. The message should be titled **Voice-mail from *xxxx*** and include the voice mail as a `.wav` attachment.

To check Message State Change Notification

1. Log in to extension 1000's voice mail from a phone. The message you left in the preceding step should be there as a new message.
2. Save the message by pressing 3. Within approximately a minute, the message in Outlook will become a saved message as well—it will no longer appear in **bold**.

To Listen to VM in Outlook

Open the message in Outlook, and open the `.wav` attachment. It should be the same message.

To check Deletion Notification

1. Delete this message from Outlook.
2. Wait a couple of minutes, and then log on to extension 1000's voice mail from a phone. The voice mail should no longer be there.

If any of these tests fail, consult the "Troubleshooting Tips" section.

Troubleshooting Tips

To check the profile for the service account

1. Log on to the MaxACD system as the *AltiGen service account* (for example, **AltiGen_telesystem**). You will need the password you set up when you installed MaxACD.
2. Select **Control Panel > Mail**. (In Windows 2003, right-click **Microsoft Office** on the **Start** menu, and select **Properties**.)
3. Click **Show Profiles**. In MaxACD, there is only one profile there, which is for the service account, so that name should be AltiExch<*ServerName*><*AccountName*> (for example, AltiExchMAILSERVERAltiGen_telesystem).

   If you don't see any such profile, make sure that \altiserv\exe folder does not contain the files **`mapi32.dll`** or **`gapi32.dll`**. If these files exist, delete them, then stop and start the Exchange Integration Service.

To delete the profile for the service account

If an error occurred while MaxACD was creating the service account profile, the damaged profile would remain there until removed manually. After the reconfiguration, the new profile can't be created, because the old one still exists.

You can remedy this in the following way:

1. Log on as AltiGen Service Account.
2. Shut down Altigen VM Exchange Integration Service from **Control Panel > Administrative Tools > Services**, then open **Control Panel > Mail** (or **Mail and Fax**) and click **Show Profiles**. Remove the service profile.
3. Start the **AltiGen VM Exchange Integration Service** from **Control Panel > Administrative Tools > Services**.

If this doesn't work, contact AltiGen Technical Support.

To gather trace files

1. Log in to MaxACD Administrator, first with the password "jazzy" and then with your own Admin password.
2. Select **Turn AltiTrace On**, and click **Apply**.
3. Select **VM and SP Log Dump**.
4. To view logs, go to AltiServ\Log\VM\ExchIntg.

To avoid "extension in use" message

When synchronizing with Exchange Server, the mailbox needs to be locked. If the extension has a lot of messages, it could take some time, but shouldn't take as long as 2-3 minutes. In normal cases, it should take just 10-20 seconds. You may adjust a registry key to change the synchronization interval:

```
HKEY_LOCAL_MACHINE\SOFTWARE\AltiGen Communications,
Inc.\AltiWare\ExchIntg\Polling Interval
```

The value is in ms. 60000 = 60 seconds. You may change it to 300000 for 5 minutes. After changing the value, restart Exchange integration service for the change to take effect.

Exchange Integration service synchronizes voice messages on the Exchange server with those on the MaxACD system by polling the two servers periodically. This polling interval can be adjusted by creating a DWORD value called "Polling Interval" under the key

```
HKEY_LOCAL_MACHINE\SOFTWARE\AltiGen Communications,
Inc.\AltiWare\ExchIntg
```

This DWORD value should contain the number of milliseconds between polling. If this value is not present in the registry, a default value of 60000 (1 minute) is used by the system. For performance reasons, you should not set this value to below 60000.

To avoid "Access Deny" error while sending messages

If you have applied Microsoft patch ms06-029, when a MaxACD phone user attempts to send a message, the user receives an "Access Deny" error. This is because the patch changes the grant for the permission of **Send As**.

After applying the patch, the **Send As** permission of each user needs to be granted to the account of "altigen service" explicitly.

You may have to restart the Exchange Server and MaxACD.

Notes

- Prevent attempts by the Exchange Administrator/Manager to use the existing service account for the AltiGen Exchange Integration Service. Using the service account will provide an audit trail that is invaluable while troubleshooting.
- Depending on the number of voice mails you have on the MaxACD server, the initial mailbox synchronization may take a long time.

  For example, if you have 10GB of voice mails on the MaxACD server and are enabling Exchange integration for all the mailboxes, it may take up to 24 hours to initialize the Exchange integration service.

  If you have less than 100MB of voice mails on the MaxACD server, the initialization will take less than 5 minutes.

- If users experience a problem making calls to the Exchange server, make sure the MSXML 6.0 Parser has not been deleted from the server. Without it, the speech engine services cannot play voice prompts.

CHAPTER

23

Tools and Applications

MaxACD comes with the following tools and applications for testing, diagnosing and configuring your system. They are available from the Windows **Start** menu: **Start > All Programs > MaxACD for Lync**.

Under **Utilities**:

- Backup and Restore Utility
- MaxACD Administrator and Extension Security Checker
- Start and Stop All MaxACD Services
- Trace Collector
- Voice File Converter
- Read Config

In addition, on the **Services > Utilities** menu in MaxACD Administrator:

- Utilities for importing and exporting extensions from/to a .csv file and for importing extensions from Active Directory

Under **HMCP Tools:**

- HMCP Configuration (For information on this tool, see “HMCP Configuration Tool” on page 56.)

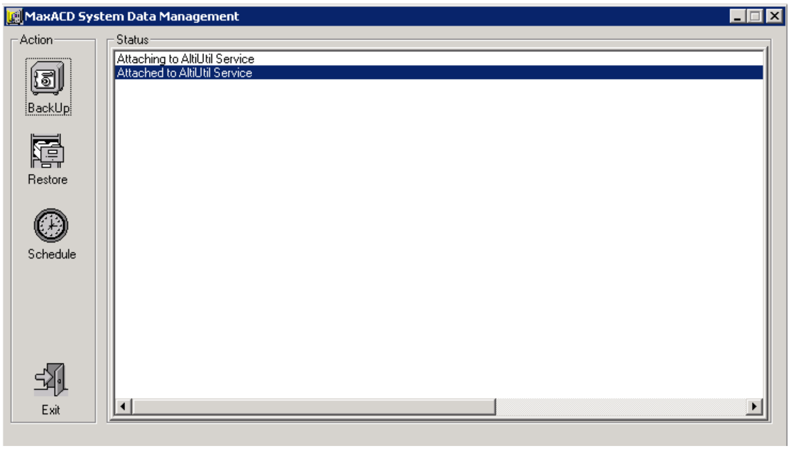
If you installed AltiGen’s Custom Phrase Manager, it is available off the **Start > All Programs** menu. You can use this tool only if you have an AltiGen SDK license.

Backup and Restore Utility

Note: The configuration backup option is turned on by default.

To back up or restore data, select either

- From MaxACD Administrator: **Services > Utilities > System Data Management**, or
- From the Windows Start menu: **All Programs** > **MaxACD for Lync** > **Utilities** > **Backup and Restore**.



Attaching to AltiUtil Service
Attached to AltiUtil Service

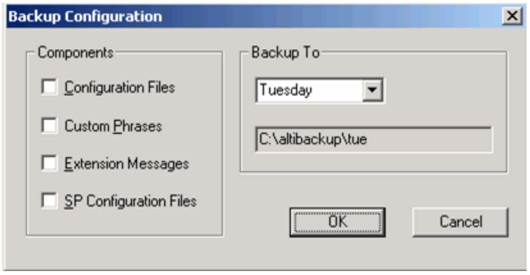
Figure 23-1. System Data Management window

Note: The System Data Management window can only be accessed at the primary MaxACD system; it is *not* available from a remote MaxACD Administrator client.

Backing Up Files

To back up files

1. Select the **Backup** icon to view the **Backup Configuration** dialog box.



☐ Configuration Files
☐ Custom Phrases
☐ Extension Messages
☐ SP Configuration Files

Backup To: Tuesday
C:\altibackup\tue

Figure 23-2. Backup Configuration dialog box

2. In the **Components** panel, select the files you want to back up.
3. In the **Backup To** drop-down list, select the day of the week (each day has its own folder in C:\altibackup for backing up files to), or select **Advanced** to change the drive or select a different folder.

   Selecting **Advanced** displays a folder icon. Click the folder icon to open a browse dialog box that lets you select the folder to back up to. When you click **OK** in the dialog box, the selected drive or directory is displayed in the field below the **Backup To** drop-down list.
4. Click **OK** to start the backup.

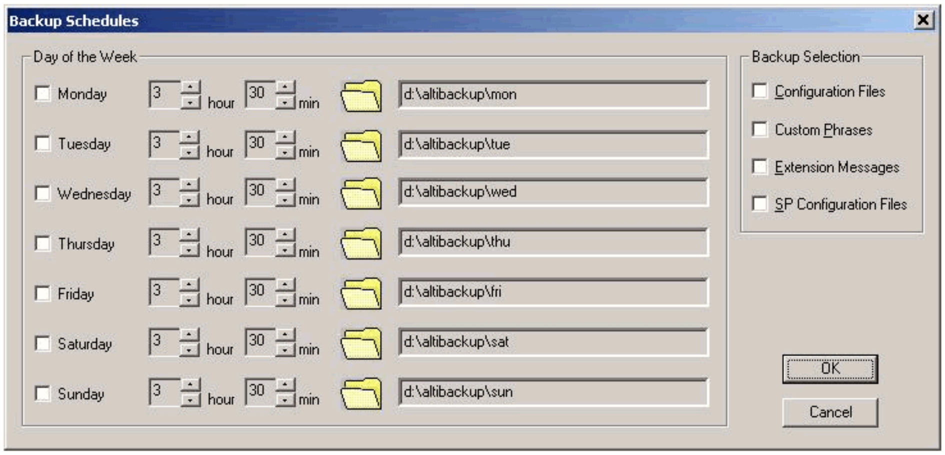
   In the window, the progress and status of the file backup is displayed.

Scheduling Backups

You can set up automated backup on a schedule, and you can select the days, the times, and the target drives and folders for the backups.

To set backup schedules

1. In the System Data Management window, select the **Schedule** button.



Backup Schedules

Day of the Week

☐ Monday	3 hour	30 min	d:\altibackup\mon
☐ Tuesday	3 hour	30 min	d:\altibackup\tue
☐ Wednesday	3 hour	30 min	d:\altibackup\wed
☐ Thursday	3 hour	30 min	d:\altibackup\thu
☐ Friday	3 hour	30 min	d:\altibackup\fri
☐ Saturday	3 hour	30 min	d:\altibackup\sat
☐ Sunday	3 hour	30 min	d:\altibackup\sun

Backup Selection

☐ Configuration Files
☐ Custom Phrases
☐ Extension Messages
☐ SP Configuration Files

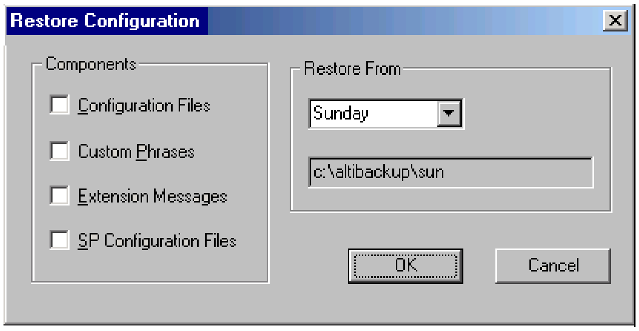
Figure 23-3. Backup Schedules dialog box

2. Set the options:
   - Check the box for each day of the week you want run the backup.
   - For each day, use the lists to specify the time. These time settings use a 24-hour clock.
   - You can accept the default target directories or click the **Folder** icon to open the **Browse for Folder** dialog box to select the destination for the backup files.
   - Under **Backup Selection**, select the file components you want to back up: Configuration files, Custom Phrases, Extension Messages, SP Configuration files.
3. Click **OK**.

Restoring Backed up Files

To restore backed up files

1. Stop the MaxACD switching services.
2. In the System Data Management window, click the **Restore** button to view the **Restore Configuration** dialog box.



Restore Configuration

Components

- ☐ Configuration Files
- ☐ Custom Phrases
- ☐ Extension Messages
- ☐ SP Configuration Files

Restore From: Sunday

c:\altibackup\sun

Figure 23-4. Restore Configuration dialog box

3. Under **Components**, select the file groups you want to restore.
4. Using the **Restore From** drop-down list, select the day you want to restore from, or select **Advanced** to choose the restore folder.

   Clicking **Advanced** displays a folder icon that you can click to open a dialog box that allows you to select the directory you want to restore from.

   Select a day of the week or manually choose the restore directory. The specified directory appears in the text box below the drop-down list.

Note: The components you select for restore must have been backed up into the directory you selected. For example, if you didn’t back up configuration files on Thursday, you won’t be able to restore them from the Thursday directory.

Important: Make sure the version you restore the database files from is compatible with the current MaxACD version. If incompatible files are restored, the system will fail to restart!

5. Click **OK** to start the restore process.
6. When you are finished restoring backed up files, restart the MaxACD switching services.

MaxACD Admin & Extension Security Checker

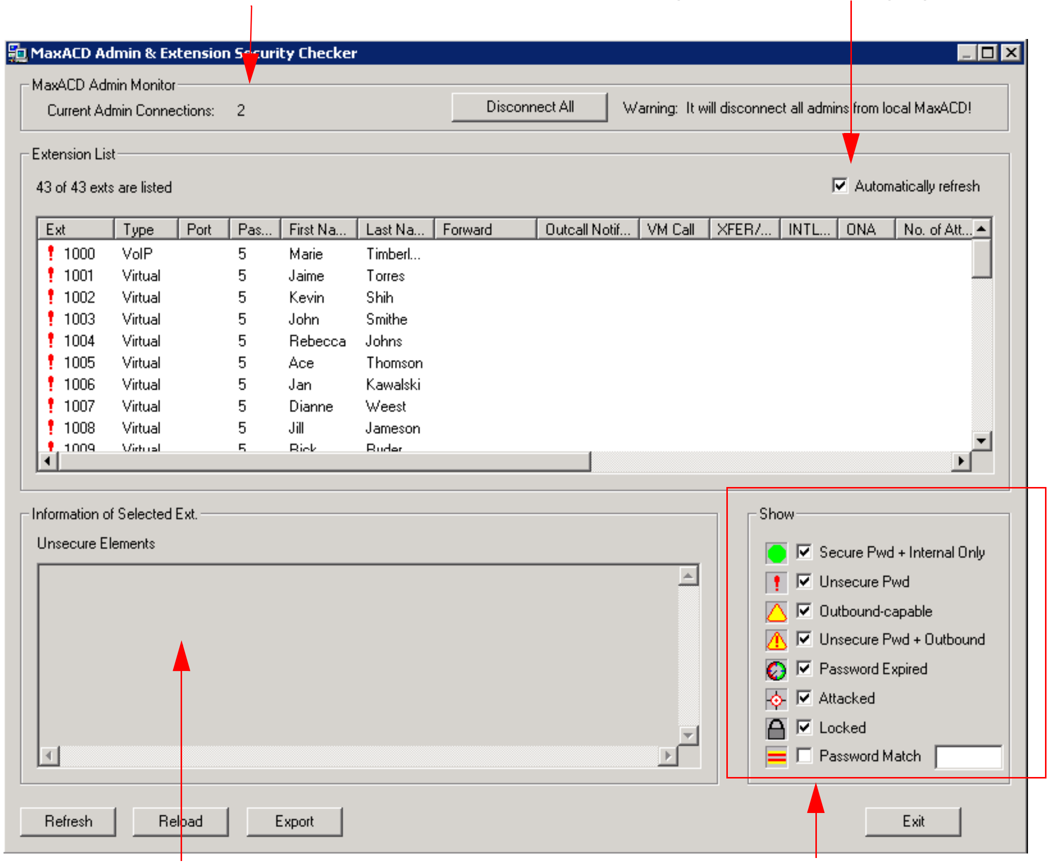
MaxACD Admin & Extension Security Checker is a tool that

- Checks the security status of every extension in your MaxACD system and displays the security characteristics of each extension. From an extension’s right-click menu, you can lock and unlock the extension, force the user to change the password, clear an attacked record, and reset the status.
- Shows how many MaxACD Administrators are currently connected to the system. By clicking **Disconnect All**, you can disconnect all Admins from the local MaxACD system.

Launch the MaxACD Administrator & Extension Security Checker from **Start** > **All Programs** > **MaxACD for Lync**> **Utilities** > **MaxACD Admin & Extension Security Checker**.

Number of Admin connections

Automatically refreshes the display



MaxACD Admin & Extension Security Checker

MaxACD Admin Monitor

Current Admin Connections: 2

Warning: It will disconnect all admins from local MaxACD!

Extension List

43 of 43 exts are listed

☑ Automatically refresh

Ext	Type	Port	Pas...	First Na...	Last Na...	Forward	Outcall Notif...	VM Call	XFER/...	INTL...	ONA	No. of Att...
! 1000	VoIP		5	Marie	Timberl...							
! 1001	Virtual		5	Jaime	Torres							
! 1002	Virtual		5	Kevin	Shih							
! 1003	Virtual		5	John	Smithe							
! 1004	Virtual		5	Rebecca	Johns							
! 1005	Virtual		5	Ace	Thomson							
! 1006	Virtual		5	Jan	Kawalski							
! 1007	Virtual		5	Dianne	Weest							
! 1008	Virtual		5	Jill	Jameson							
! 1009	Virtual		5	Rick	Ruder							

Information of Selected Ext.

Unsecure Elements

Show

- ● ☑ Secure Pwd + Internal Only
- ! ☑ Unsecure Pwd
- ⚠ ☑ Outbound-capable
- ⚠ ☑ Unsecure Pwd + Outbound
- ☑ Password Expired
- ☑ Attacked
- ☑ Locked
- ☐ Password Match

Information on the selected extension

Security characteristics to check

Figure 23-5. MaxACD Administrator & Extension Security Checker

Checking Extension Security

Generally, an extension is considered secure if its password meets the following conditions:

- Contains 4-8 digits
- Is different from the extension
- Is different from the default system password
- Does not consist of consecutive numbers
- Does not consist of a repetition of the same digit

To check extension security

1. Select the security characteristics you want to check in the **Show** field group.

Status	Description
Secure Pwd + Internal Only	Has secure password and cannot make outbound trunk calls

Status	Description
Unsecure Pwd	Password has unsecure elements described in **Unsecure Elements** window
Outbound-capable	Can make outbound trunk calls
Unsecure Pwd + Outbound	Password has unsecure elements described in **Unsecure Elements** window AND can make outbound trunk calls
Password Expired	Password is expired
Attacked	8 consecutive false password attempts have been made
Locked	Extension has been locked by system due to attack or by System Administrator
Password Match	To detect if an extension uses a specific trivial password, such as street address, zip code, phone number, enter that string here.

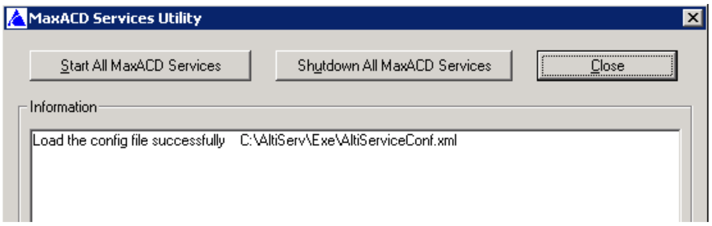
2. Click **Refresh.** Extensions with the selected insecure characteristics will appear in the Extension List.
3. Make changes to extensions from the right-click menus, or advise extension user(s) to make changes.
4. After changes have been made (for example in MaxACD Administrator or with right-click commands in this tool), click **Reload** to fetch the new settings from MaxACD.

   Security characteristics for extensions you select in the Extension List display in the Unsecure Elements panel.
5. (Optional) Click **Export** to export the data in the Extension List to a text file.

Note: You are advised to run this security check periodically and remind extension users to use secure passwords.

Start & Stop All MaxACD Services

You can start or stop all MaxACD services from the Windows **Start** menu: **All Programs > MaxACD for Lync > Utilities > Start & Stop All MaxACD Services**.



Load the config file successfully   C:\AltiServ\Exe\AltiServiceConf.xml

Figure 23-6.   MaxACD Services Utility dialog box

To shut down all MaxACD services, click the **Shutdown All MaxACD Services** button. Some examples of when you might want to do this are before you upgrade, before running some utilities and tools, and to apply certain configuration changes.

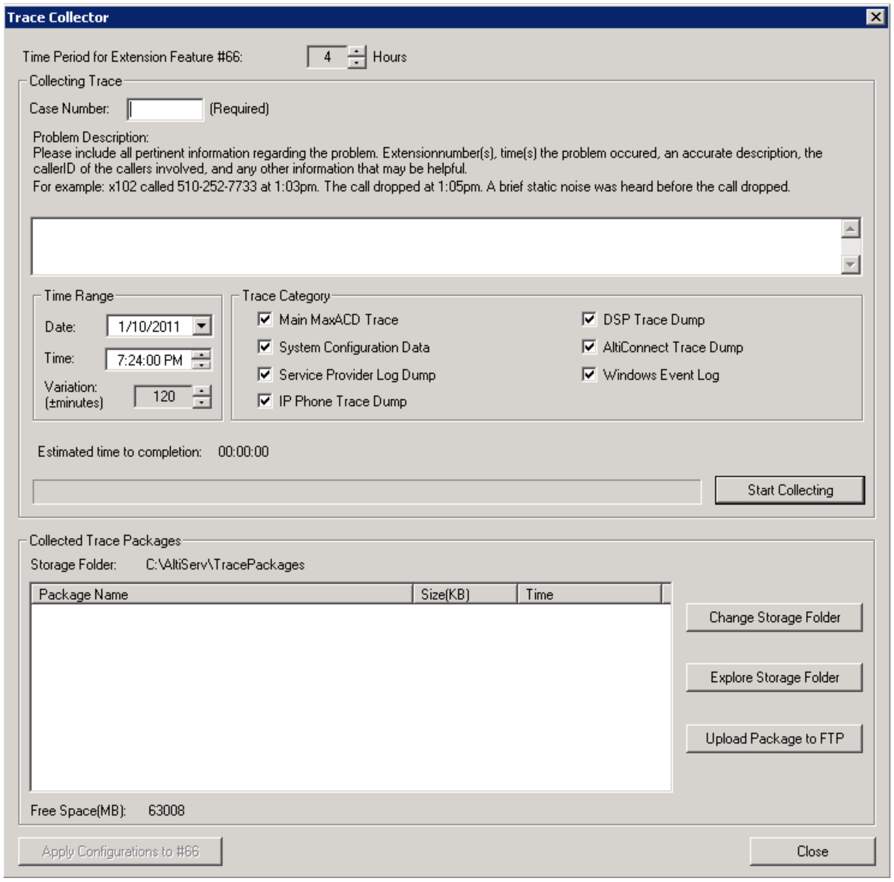
To start all MaxACD services, click the **Start All MaxACD Services** button.

Trace Collector

The Trace Collector is for use by experienced technicians. It collects trace for diagnostic purposes, and lets you upload the results to AltiGen Technical Support right from the Trace Collector dialog box. Technicians can run the Trace Collector tool from the Windows **Start** menu, and also from MaxACD Administrator's **Diagnostic** menu. Log in with the super technician password "jazzy" and then the current password when logging into MaxACD Administrator. This enables the diagnostic menu options.

Note: Trace Collector is not available from a MaxACD Administrator installed in a remote machine.

The Trace Collector first examines the running status of MaxACD and the gateway, and then checks whether each trace status is on or off. If a trace status is turned off, the MaxACD system will not produce those traces. A message box pops up if MaxACD and the gateway are not running or an important trace status is off.



Trace Collector

Time Period for Extension Feature #66: 4 Hours

Collecting Trace

Case Number: (Required)

Problem Description:
Please include all pertinent information regarding the problem. Extensionnumber(s), time(s) the problem occured, an accurate description, the callerID of the callers involved, and any other information that may be helpful.
For example: x102 called 510-252-7733 at 1:03pm. The call dropped at 1:05pm. A brief static noise was heard before the call dropped.

Time Range
Date: 1/10/2011
Time: 7:24:00 PM
Variation: (±minutes) 120

Trace Category
☑ Main MaxACD Trace
☑ System Configuration Data
☑ Service Provider Log Dump
☑ IP Phone Trace Dump
☑ DSP Trace Dump
☑ AltiConnect Trace Dump
☑ Windows Event Log

Estimated time to completion: 00:00:00

Collected Trace Packages
Storage Folder: C:\AltiServ\TracePackages

Package Name	Size(KB)	Time

Free Space(MB): 63008

Figure 23-7. Trace Collector dialog box

Following are descriptions of the fields in the Trace Collector

Time Period for Extension Feature #66: Defines how many hours you want to go back to collect trace, starting from the time you press **#66**. The default value is 2 hours.

Case Number: Enter the AltiGen case number associated with this trace collection activity. The case number will comprise the first part of the file name of the collected trace package.

Problem Description: Enter a description of the problem, including the extension number involved, the time when the problem happened, how to reproduce the problem, and so on.

Time Range: The tool collects the trace between the time ranges. The time range covers before *and* after the defined Date and Time. The default Date and Time is one hour before the current date and time, and the default variation is 60 minutes. This setting is not applicable when **#66** is performed.

Trace Category: By default, all options are selected.

- **Main MaxACD Trace** (\AltiServ\log)

  Collects the following files, and extracts the trace records that fall in the specified time range:

actrace.log	AlpErrLog.txt	SIPlog.txt
ALPxxx.txt	\atps\threadID.txtl	SIPMan.txt
altiserv.txt	\atps\cmdlog.txt	SIPPstnReg.txt
AltiBack_XXX.trc	AdvQOverflow.log	SipExtChanTbl.log
AltiKeep_XXX.trc	Ac2AppPathHdlTbl.txt	SIPKeepALive.txt
AnnouceRunLog.txt	FeatServ.txt	QESLLog.txt
AssertLog.txt	DbUpdateTrdLog.txt	
AW_AstrCpyErrLog.txt	HGwGenLog.txt	Loggservice_Mutex.txt
CallQManLog.txt	HGwMsgLog.txt	MEMORYTRACE.txt
CDRLogDLL.txt	threadid.txt	NewCDRExt.txt
CDRLogTrace.txt	MidNightLog.txt	
ConfigLog.txt	\logservice\Internal.txt	pathlog.txt
MsgOCLog.txt	ConfigServiceLog.txt	rsrclog.txt
MSRunLog.txt	CDRLogTrace.txt	RtpPortRangeTbl.txt
mviperr.txt	CDRLogDLL_EXCEPTION.txt	StartupLog.txt
Postman.txt	CSH323log.txt	Swxx_xxxx.txt
ProcInfoLog.txt	ExceptionLog.txt	GWMsgLog.txt

- **System Configuration Data**

  Collects system configuration data, including System, Extension, Trunk, AA configurations, and Read OE files.

- **Service Provider Log Dump**

  Runs SPDump.exe to dump the SP log into files and then collects the trace.

- **IP Phone Trace Dump**

  Collects the IPPhone dump log in \AltiServ\Log\IPP.

- **Stand-alone Gateway Trace**

  Collects the trace on the stand-alone gateway machine. If MaxACD Services are shut down, the option is disabled. If Trace Collector is running on the stand-alone gateway machine, this option is hidden (because Trace Collector just needs to collect the trace locally).

- **AltiConnect Trace Dump**

  Runs acdump.exe to dump the AltiConnect Trace, and then collects the trace. If Trace Collector is running on the stand-alone gateway machine, this option is hidden.

- **Windows Event log**

  Extracts the system and application event log from the Windows system.

Start Collecting: Click this button to begin the trace collection, according to the time range and trace categories you chose. All collected files will be zipped to a single file, which will be listed in the Collected Trace Packages list box. The progress bar will display the progress of the whole process.

Storage Folder: The collected trace package is saved in this folder. The format of the file name is CaseNumber_Year_Month_Day_Hour_Minute_Second _ComputerName.zip. If the trace package is collected by **#66**, the format of the file name is #66_Year_Month_Day_Hour_Minute_Second _ExtesionNumber.zip.

Free Space: Displays the free space of the drive where the storage folder is located. The folder must be in a local drive.

Change Storage Folder: Pops up a folder browser window to select another storage folder. After the change, **Storage Folder**, **Free Space**, and the package list are refreshed to reflect the status of the new storage folder.

Explore Storage Folder: Opens the storage folder in a new explorer window.

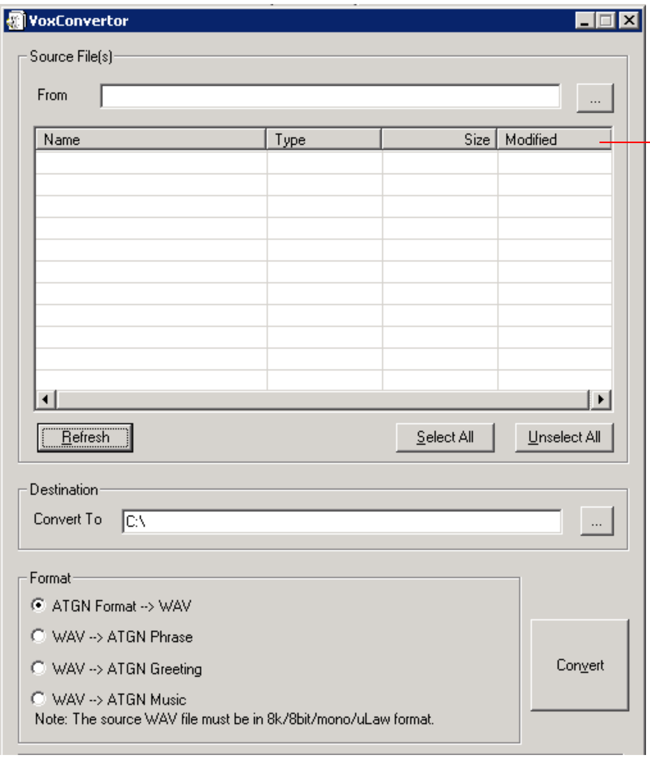
Upload Package to FTP: Opens an FTP configuration dialog box. After you complete the required configuration, Trace Collector uploads the selected package to the AltiGen Tech Support FTP site.

Apply Configurations to #66: Apply time period, trace category, and storage folder to feature code #66 (Trace Collecting).

Voice File Converter

This tool converts phrase, greeting, and music files from .wav to AltiGen format and vice versa. To open the tool, from the Windows **Start** menu, select **All Programs > Utilities > Voice File Converter**.

Note: The source .wav file must be in 8k/8bit/mono/mu-law format.



Convert To: C:\

● ATGN Format --> WAV
○ WAV --> ATGN Phrase
○ WAV --> ATGN Greeting
○ WAV --> ATGN Music

Note: The source WAV file must be in 8k/8bit/mono/uLaw format.

You can sort by clicking a column head

Figure 23-8. Voice Converter dialog box

To use the Voice File Converter:

1. Beside the **From** field, click the Browse button to select the folder that contains the files you want to convert.
2. Beside the **Convert To** field, click the Browse button to select the destination folder for the converted files. If they are prompts, they should be placed in the **C:\PostOffice\phrases\LangCustom** directory on the gateway that is running MaxACD. If the files are music files, they should be placed in the **C:\PostOffice\Phrases\Music** directory. A file that you want to use for music on hold must be named MusicOnWaiting. To save the MaxACD system MusicOnWaiting file, rename it before replacing it.
3. Check the files you want to convert.
4. In the Format panel, select a format.
5. Click **Convert**.

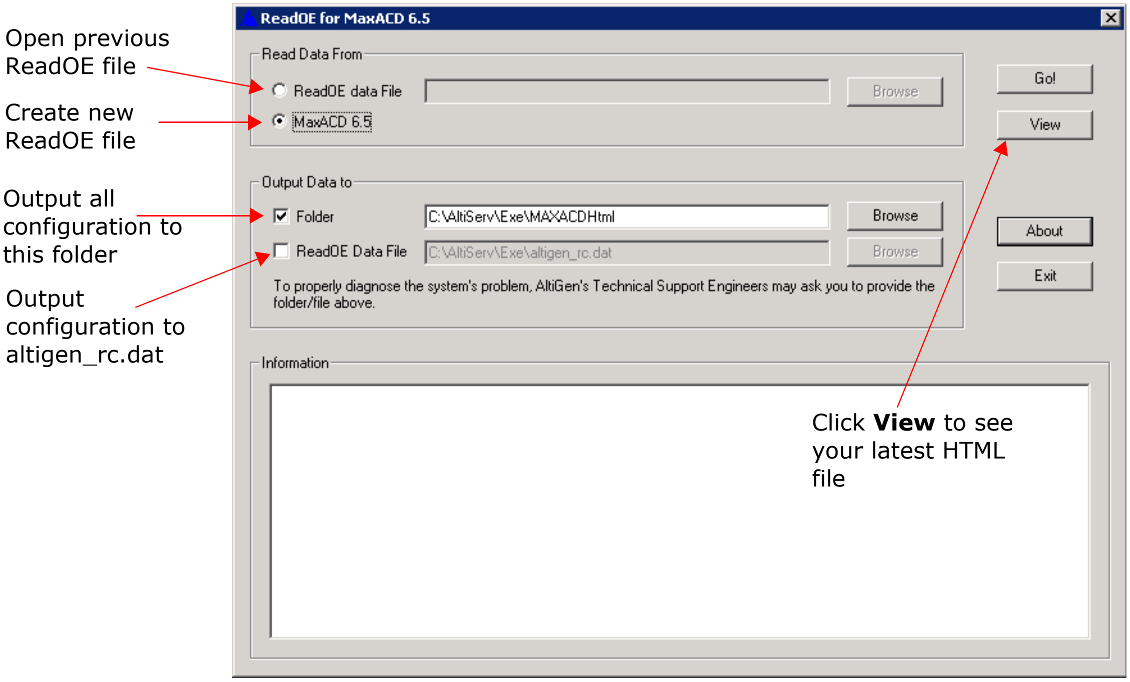
If a file format is incorrect, an error message appears.

Read Config

Read Config (or Configuration Reader) is a tool that creates a subdirectory in \altiserv\EXE\AltiWareHtml\ of HTML files showing details of your MaxACD configuration.

To use Configuration Reader

1. Launch Configuration Reader from **Start > All Programs > MaxACD for Lync > Utilities > Read Config**.



Read Data From:
○ ReadOE data File
● MaxACD 6.5

Output Data to:
☑ Folder C:\AltiServ\Exe\MAXACDHtml
□ ReadOE Data File C:\AltiServ\Exe\altigen_rc.dat

To properly diagnose the system's problem, AltiGen's Technical Support Engineers may ask you to provide the folder/file above.

Open previous ReadOE file

Create new ReadOE file

Output all configuration to this folder

Output configuration to altigen_rc.dat

Click **View** to see your latest HTML file

Figure 23-9. ReadOE dialog box

2. Make selections in the dialog box. If you will be sending a configuration file to AltiGen Technical Support, check **ReadOE Data File**, and select a folder for the .dat file.
3. Click **Go**.

   A processing bar indicates the progress of configuration reading.
4. When the status window is complete, you can click the **View** button to view the HTML files showing your configuration.

Columns across the top of the opening page let you view statistics on different components of your configuration.

Exporting and Importing Extensions

You can import and export extensions in a .csv file and you can import extensions from the active directory.

Importing Extensions from a .csv File

1. First, back up your system configurations, using AltiGen’s System Data Management tool (**Services > Utilities > System Data Management**).
2. Go to **Services > Utilities > Import Extensions**.

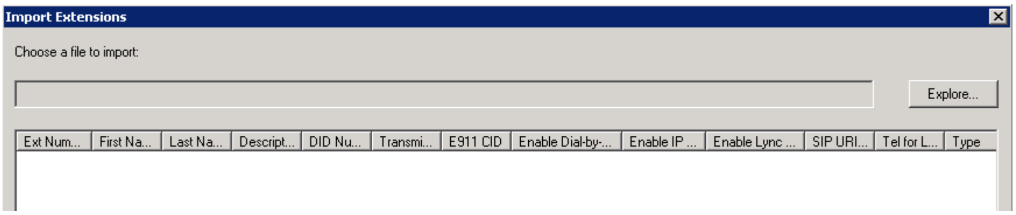


Figure 23-10. Import Extensions dialog box

3. In the Import Extensions dialog box, click the **Explore** button to select a .csv file to import, and click **OK**.

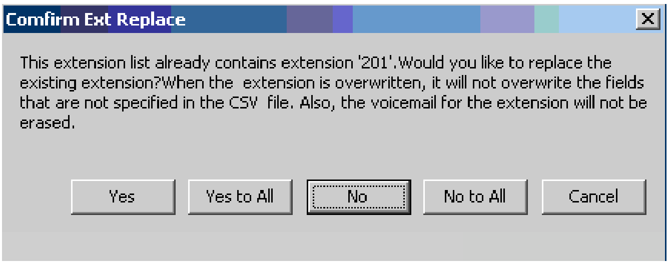
   All the extension records in the .csv file are added to the Import Extensions list.

4. Check the records you want to import. Click the **Select All** and **Clear All** buttons to select or clear all the check boxes.)

5. Click **Import**.

   A progress bar lets you see the progress of the import. When the import is finished, a message lets you know how many extensions were imported, how many extensions were skipped and how many extensions failed.

6. If an extension already exists, a dialog box pops up asking if you want to replace the extension:

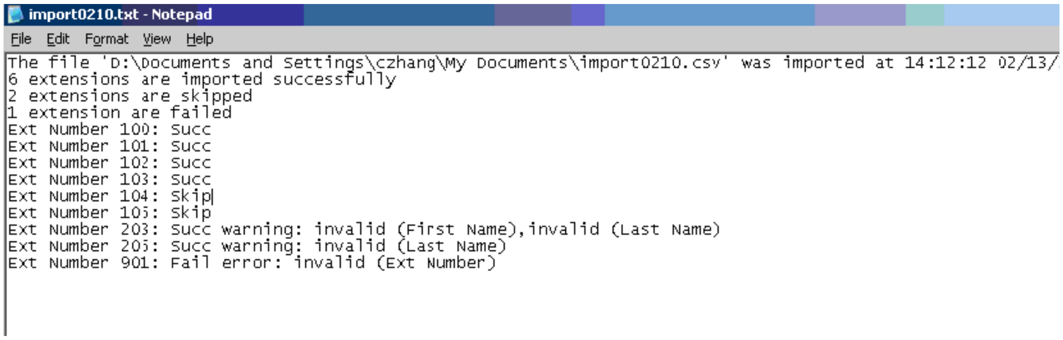


This extension list already contains extension '201'.Would you like to replace the existing extension?When the extension is overwritten, it will not overwrite the fields that are not specified in the CSV file. Also, the voicemail for the extension will not be erased.

Figure 23-11. Confirm replacement prompt

If you overwrite an extension, fields that are not specified in the .csv file are not overwritten with default values or blank values. For example, if the column **Department** is not included in the .csv file, but is configured in the extension that you overwrote, the **Department** field is not reset to the default value when the extension is overwritten.

When the import is finished, a report file opens showing detailed information for every extension you attempted to import. If some fields are invalid, the system replaces them with a default value, except for the extension number field.



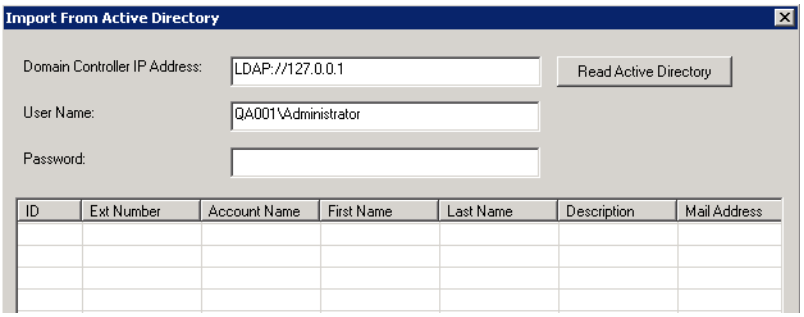
```
The file 'D:\Documents and Settings\czhang\My Documents\import0210.csv' was imported at 14:12:12 02/13/
6 extensions are imported successfully
2 extensions are skipped
1 extension are failed
Ext Number 100: Succ
Ext Number 101: Succ
Ext Number 102: Succ
Ext Number 103: Succ
Ext Number 104: Skip
Ext Number 105: Skip
Ext Number 203: Succ warning: invalid (First Name),invalid (Last Name)
Ext Number 205: Succ warning: invalid (Last Name)
Ext Number 901: Fail error: invalid (Ext Number)
```

Figure 23-12. Report showing the extension import

The name of the text file is the same as the .csv file, except that the file extension is .txt.

Importing Extensions from the Active Directory

1. First, back up your system configurations, using AltiGen's System Data Management tool (**Services > Utilities > System Data Management**).
2. Go to **Services > Utilities > Import Extensions from Active Directory**.



Domain Controller IP Address: LDAP://127.0.0.1

User Name: QA001\Administrator

Password:

ID	Ext Number	Account Name	First Name	Last Name	Description	Mail Address

Figure 23-13. Import from Active Directory dialog box

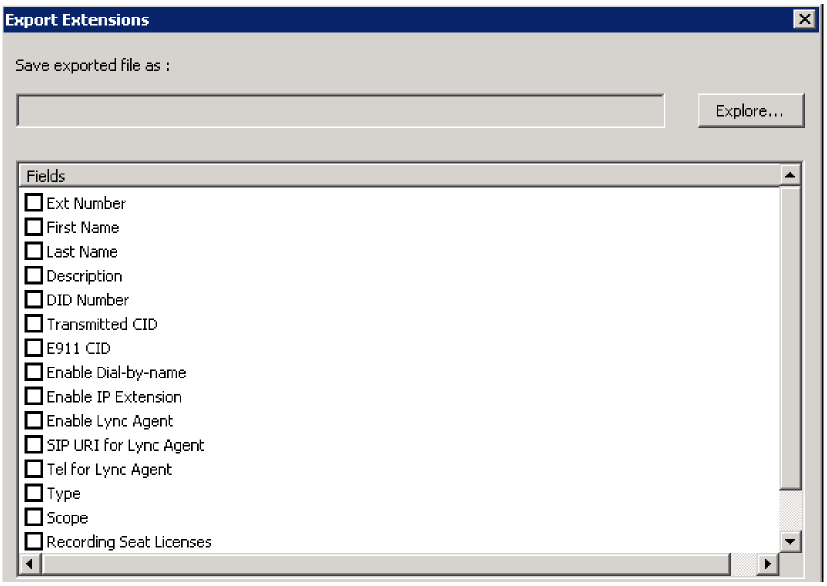
3. Enter the server path, user name and password.
4. Click the **Read Active Directory** button.

   All user information is displayed in the table. (A record must have either an Ext Number or First Name or Last Name or Mail Address, otherwise it will not be not listed in the table.)
5. Select the extensions you want to import. You can use the **Select All** button, but only records that have an extension number can be selected. If an extension number is empty, a warning message appears.
6. You can use the **Clear All** button to clear all checkmarks.
7. Click **Import**. A progress bar tells you the progress of importing.
8. If an extension already exists in the destination list, a dialog box opens.
9. Respond to the question in the dialog box. If you decide to overwrite the extension, other fields not in the Active Directory are kept.

After finishing importing, a dialog box tells you how many extensions were imported successfully. When you click **OK**, an error report file is opened automatically to tell you the detailed information on every extension. If some fields are invalid, the system replaces them with a default value (except for the extension number). (The report file's name is "ReportImportAD.txt". It is in the \altiserv\exe directory.)

Exporting the Extensions in a MaxACD System

1. Go to **Services > Utilities > Export Extensions**.



- □ Ext Number
- □ First Name
- □ Last Name
- □ Description
- □ DID Number
- □ Transmitted CID
- □ E911 CID
- □ Enable Dial-by-name
- □ Enable IP Extension
- □ Enable Lync Agent
- □ SIP URI for Lync Agent
- □ Tel for Lync Agent
- □ Type
- □ Scope
- □ Recording Seat Licenses

Figure 23-14. Export Extensions dialog box

2. Click **Explore** and specify a name and location for the .csv file you’re about to create.
3. Check the fields you want to export. Use the **Select All** and **Clear All** buttons to select or clear all the check boxes.

   Note: You must export the extension number field.
4. Click **Export** to save the extension configurations to a .csv file. A progress bar indicates how many extensions were exported.

Editing a .csv File

If you edit a .csv file,

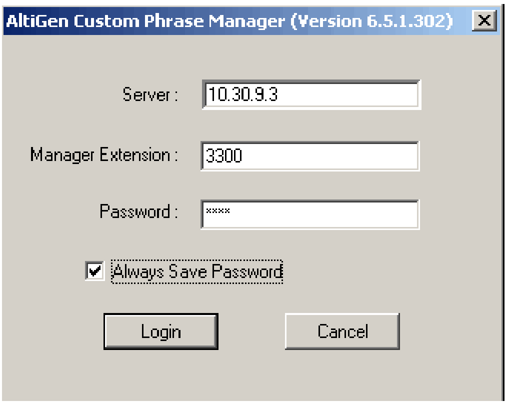
- All fields must be separted by a "," and all the records must be divided by pressing the **Enter** key.
- The first line must be a pre-defined field name, such as “First Name”. If the field name doesn’t match a pre-defined field name, the field is skipped during an import operation.
- The sequence of the columns doesn’t matter.

AltiGen Custom Phrase Manager

The AltiGen Custom Phrase Manager is a Windows-based application that makes managing custom phrases easy. It displays all custom phrases in a graphical user interface. You can add or delete a phrase by clicking a button. You also can rename an existing phrase to a meaningful name, rather than pressing digits on the telephone.

Note: The AltiGen Custom Phrase Manager requires a Client SDK license.

To use the AltiGen Custom Phrase Manager, open the tool from the Windows **Start > All Programs** menu.



AltiGen Custom Phrase Manager (Version 6.5.1.302)

Server : 10.30.9.3

Manager Extension : 3300

Password : ****

☑ Always Save Password

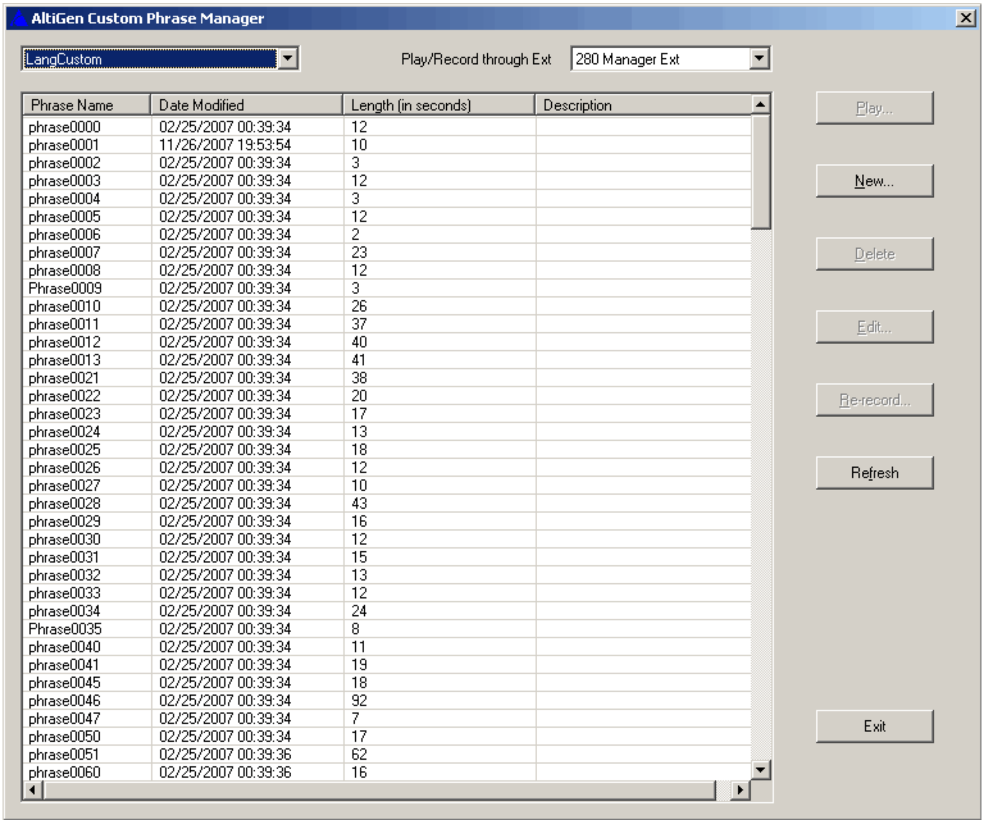
Figure 23-15. Custom Phrase Manager dialog box

Enter the following information and then click **Login**:

- MaxACD server address
- Manager Extension
- Manager Extension password.

If you want to save the password for this application, check the **Always Save Password** box.

Note: The server address and the extension number will be written to the windows registry. If you choose **Always Save Password**, the password will be encrypted and also saved in the registry. The tool will automatically reload the server address, manager extension number and the password from the registry when it starts next time.



LangCustom

Play/Record through Ext: 280 Manager Ext

Phrase Name	Date Modified	Length (in seconds)	Description
phrase0000	02/25/2007 00:39:34	12	
phrase0001	11/26/2007 19:53:54	10	
phrase0002	02/25/2007 00:39:34	3	
phrase0003	02/25/2007 00:39:34	12	
phrase0004	02/25/2007 00:39:34	3	
phrase0005	02/25/2007 00:39:34	12	
phrase0006	02/25/2007 00:39:34	2	
phrase0007	02/25/2007 00:39:34	23	
phrase0008	02/25/2007 00:39:34	12	
Phrase0009	02/25/2007 00:39:34	3	
phrase0010	02/25/2007 00:39:34	26	
phrase0011	02/25/2007 00:39:34	37	
phrase0012	02/25/2007 00:39:34	40	
phrase0013	02/25/2007 00:39:34	41	
phrase0021	02/25/2007 00:39:34	38	
phrase0022	02/25/2007 00:39:34	20	
phrase0023	02/25/2007 00:39:34	17	
phrase0024	02/25/2007 00:39:34	13	
phrase0025	02/25/2007 00:39:34	18	
phrase0026	02/25/2007 00:39:34	12	
phrase0027	02/25/2007 00:39:34	10	
phrase0028	02/25/2007 00:39:34	43	
phrase0029	02/25/2007 00:39:34	16	
phrase0030	02/25/2007 00:39:34	12	
phrase0031	02/25/2007 00:39:34	15	
phrase0032	02/25/2007 00:39:34	13	
phrase0033	02/25/2007 00:39:34	12	
phrase0034	02/25/2007 00:39:34	24	
Phrase0035	02/25/2007 00:39:34	8	
phrase0040	02/25/2007 00:39:34	11	
phrase0041	02/25/2007 00:39:34	19	
phrase0045	02/25/2007 00:39:34	18	
phrase0046	02/25/2007 00:39:34	92	
phrase0047	02/25/2007 00:39:34	7	
phrase0050	02/25/2007 00:39:34	17	
phrase0051	02/25/2007 00:39:36	62	
phrase0060	02/25/2007 00:39:36	16	

- The drop-down list at the top left displays all the directories of custom phrases under your MaxACD system's PostOffice\phrases\ directory, such as LangCustom, LangCustom_Chinese, Tenant1Custom.
- The drop-down list at the top right lets you select an extension through which to record or listen to a phrase.
- The table shows all custom phrases under the selected directory, including:
    - Phrase name
    - Date and time the phrase was created or last modified
    - Phrase length
    - A column for a description of the phrase

  Data can be sorted in ascending or descending order by clicking a column heading.
- Buttons let you play, create and edit phrases.

Creating New Phrases

To create a new phrase,

1. Select the extension you will be using to record the phrase.
2. Click **New**.

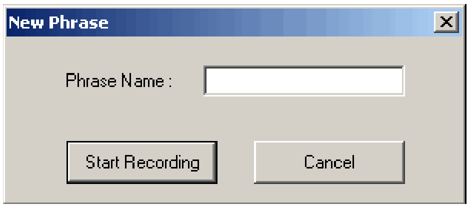


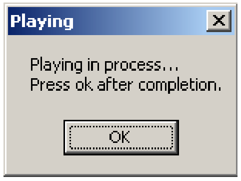
Figure 23-16. New Phrase dialog box

3. Enter a name for the phrase.
4. Click **Start Recording**.
5. After you finish recording, press **#** on the phone and follow the instructions you hear. Also click **OK** in the dialog box onscreen when done.

Playing a Phrase

To play a phrase,

1. Select the extension you will be using to listen to the phrase.
2. Click the **Play** button. The extension will ring.
3. Answer the ring, and a voice announces the phrase before playing it.



Playing in process...
Press ok after completion.

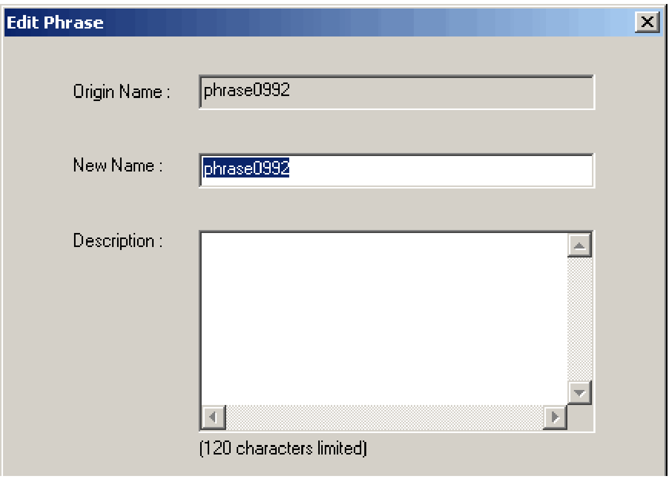
Figure 23-17. Playing a Phrase dialog box

4. After you finish listening, hang up the phone and click **OK** in the AltiGen Custom Phrase Manager.

Editing a Phrase Name or Description

To edit the name of a phrase or its description,

1. Select the phrase you want to edit.
2. Click **Edit**.



Origin Name : phrase0992

New Name : phrase0992

Description :

(120 characters limited)

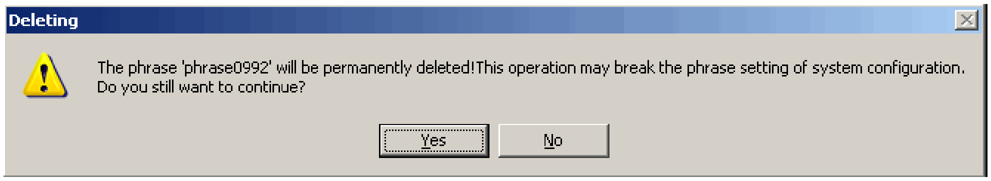
Figure 23-18. Edit Phrase dialog box

3. Make your changes to the name and description, and then click **OK**.

To Delete a Phrase

To delete a phrase,

1. Select the phrase you want to delete.
2. Click the **Delete** button. A confirmation/warning opens.



The phrase 'phrase0992' will be permanently deleted!This operation may break the phrase setting of system configuration. Do you still want to continue?

Figure 23-19. Warning message indicates the ramifications of deleting the phrase

3. If you’re sure you want to delete the phrase, click **Yes**. The phrase is deleted from the directory and from the table in AltiGen Custom Phrase Manager.

To Re-record a Phrase

To re-record a phrase,

1. Select the extension you will be using to re-record the phrase.
2. Select the phrase and click **Re-record**.
3. Click **Re-Record**.
4. When finished recording, press **#** on the phone and follow the instructions you hear. Also click **OK** in the dialog box onscreen when done.

APPENDIX

A

Network Ports

If MaxACD for Lync is behind a firewall/NAT router, you need to open TCP and UDP ports according to the following table:

For external VoIP connection through a firewall	**TCP**	**UDP**
VoIP RTP Port (Voice Stream) for SIP		From X to Y (See note below)
SIP Tie Trunk from another MaxACD server		10060
SIP Trunking Service from carrier		5060
H.245 (Media Capability)	1720 From X to Y (See note below)	

Note: An easy way to find out the RTP/TCP port range(s) for SIP is to look in MaxACD Administrator **View > Current Resource Statistics**. All the ports are listed in the **Local Ports** column.

Alternatively, you can figure the port range in the following way:

When MaxACD is running on a non-Windows 2008 system,
BasePort = 49152

When MaxACD is running on a Windows 2008 system,
BasePort = 49664 (This is because Windows 2008 has some system services use ports in the 49152 range.)

For a *single* chassis system:

X = BasePort

Y = BasePort + Total IP codec channels x 2

For a *multi*-chassis system, you need to enter multiple ranges:

Gateway ID = 0

X0 = BasePort

Y0 = BasePort + Total IP codec channels in GW0 x 2

Gateway ID = 1

X1 = BasePort + 512 x 1

Y1 = X1 + Total IP codec channels in GW1 x 2

Gateway ID = 2

X2 = BasePort + 512 x 2

Y2 = X2 + Total IP codec channels in GW2 x 2

Gateway ID=n

X(n)=BasePort + 512 x n

Y(n)=X(n) + Total IP codec channels in GW(n) x 2

To connect the following applications through a firewall	TCP	UDP
MaxAgent VM service for MaxAgent	10025 10026 10028	
MaxSupervisor	10025 10027 10028 10029 10050	
Client Applications Auto Update	10050	
Remote MaxACD Administrator	10068	
VRManager (VRManager may not work behind NAT)	10040	
Network Assessment Tool	10010	

MaxACD connects the following application through a firewall	TCP	UDP
External CDR Logger Service	10027	

APPENDIX

B

Technical Support

This appendix describes AltiGen technical support policy and procedures

Eligibility: AltiGen provides technical support to Authorized AltiGen dealers and distributors only.

End user customers, please contact your Authorized AltiGen Dealer for technical support.

How To Reach AltiGen Technical Support

Authorized AltiGen dealers and distributors may contact AltiGen technical support by any of the following methods:

- You may request technical support on AltiGen's dealer web site, at https://dealer.altigen.com. Open a case on this site, and a Technical Support representative will respond within one business day.
- Call 888-ALTIGEN, option 5, or 408-597-9000, option 5, and follow the prompts. Your call will be answered by one of AltiGen's Technical Support Representatives or routed to the Technical Support Message Center if no one is available to answer your call.

  Technical support hours are 5:00 a.m. to 5:00 p.m., PT, Monday through Friday, except holidays.

  If all representatives are busy, your call will be returned in the order it was received, within four hours under normal circumstances. Outside AltiGen business hours, only urgent calls will be returned on the same day (within one hour). Non-urgent calls will be returned on the next business day.

  Please be ready to supply the following information:

  - Dealer ID
  - AltiGen Certified Engineer ID
  - Product serial number
  - AltiWare or MAXCS version number
  - Number and types of boards in the system
  - Server model
  - The telephone number where you can be reached
  - A brief description of the problem and the procedure to reproduce the problem

Having this information ready will help us to better assist you.

Index